TIL TECHNOLOGIES
by HIRSCH

CUBE Einbruch und Übertragung Benutzerhandbuch

Dokumentnummer: GU-10023-DE
Veröffentlichungsdatum: 01/08/2024

CUBE Einbruch und Übertragung Benutzerhandbuch

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Vorwort

1. Benötigtes Material

Netzwerk für Zutrittskontrolle und Einbruchüberwachung auf der Basis von *TILLYS* **TILLYS24-CUBE**.

Wandterminal bestehend aus einem Einbruchsterminal TACTILLYS-IP CUBE **CDA00TY2025-BBIP** mit Lesegerät **LEC05XF0200-NB6**.

2. Software-Version

Diese Anleitung beschreibt, wie Sie die CUBE Einbruchfunktion für die MICROSESAME **Softwareversion 2024.2** installieren, konfigurieren und in Betrieb nehmen.

Firmware des TILLYS CUBE **ab 7.0.0**.

Firmware des TACTILLYS-IP **ab 7.0.0**.

3. Kontext für die Verwendung dieses Handbuchs

Der IT-Verantwortliche des Standorts (DSSI) des Kunden wurde vorab informiert und führte die notwendigen Maßnahmen zur Sicherung des Datenaustauschs über IP durch.

Der Sicherheitsbeauftragte hat seine Spezifikation an den TIL TECHNOLOGIES-Partner oder -Installateur weitergeleitet.

Der TIL TECHNOLOGIES Partner oder Installateur konfiguriert die TILLYS gemäß der Spezifikation in seinen Räumlichkeiten und kopiert diese Konfiguration auf einen USB-Stick. Am Standort des Kunden lädt er diese Konfigurationen auf die TILLYS, dann schließt er über MICROSESAME die TACTILLYS-IP CUBE-Terminals an, konfiguriert sie und testet ihren Betrieb.

Der Kunde nutzt die Funktionen seines/seiner TACTILLYS-IP CUBE-Terminals, um seine Gruppen scharf oder unscharf zu schalten, und die Einbruchsfunktionen werden an den Fernüberwachungsmonitor weitergeleitet.

Der Fernüberwachungsmonitor verwaltet die Alarme aus der Ferne über sein Terminal.

4. Siehe auch

- *Video zur Vorstellung des CUBE Einbruchmelders*.
- *Technisches Datenblatt zum TACTILLYS-IP CUBE Einbruch-Terminal*.
- *Schnellstartanleitung (GD-10001-DE)*.

5. Eigentumsvorbehalt

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden.

TIL TECHNOLOGIES kann nicht für die in diesem Dokument beispielhaft angegebenen Informationen verantwortlich gemacht werden. Die in den Beispielen verwendeten Organisationen, Namen und Daten sind fiktiv, sofern nicht anders angegeben.

Alle genannten Warenzeichen sind eingetragene Warenzeichen ihrer jeweiligen Eigentümer.

Kein Teil dieses Dokuments darf ohne ausdrückliche Genehmigung von TIL TECHNOLOGIES in irgendeiner Form oder mit irgendwelchen Mitteln verändert, vervielfältigt oder übertragen werden.

Senden Sie Ihre Kommentare, Korrekturen und Anregungen zu diesem Handbuch an *documentation@til-technologies.fr*.

6. Glossar

Die in diesem Handbuch verwendeten Fachbegriffe werden im Folgenden erläutert.

Alarm	Eigenschaft, die ein anormales Ereignis (Einbruch, technischer Defekt, TZLO...) meldet. Ein technischer Alarm wird rund um die Uhr überwacht und geht in den Alarm über, sobald er in die aktive Stufe wechselt. Eine Melderinformation vom Typ Einbruchalarm wird überwacht, wenn die zugehörige Meldergruppe überwacht wird. Der Übergang in den Alarm wird daher nicht nur durch ihren Übergang in den aktiven Zustand bestimmt, sondern auch durch den Überwachungsstatus ihrer Gruppe.
Auswurf	Maßnahme, um einen oder mehrere Einbruchmelder, die sich im Fehlerzustand befinden, von der Überwachung auszuschließen, damit eine Gruppe trotzdem überwacht werden kann oder um das Auslösen von Alarmen zu verhindern. Es können verschiedene Arten des Auswurfs eingestellt werden: manueller Auswurf, automatischer Auswurf, mit oder ohne automatische Rückführung oder Dauerbenutzer.
Authentifizierung	1. **Im Allgemeinen** besteht die Authentifizierung in der Eingabe von ID-Mitteln (Login / Passwort) für den Zugang zu einem Gerät wie die TILLYS, zu einer Anwendung wie CHECKPOINT für die Nutzung des Terminals MOBILIS 3 oder auch zu einem Teil oder der Gesamtheit einer Software wie bei MICROSESAME oder KSM.

2. In den Einstellungen der**Kodierung von MICROSESAME** ist Authentifizierung ein Vorgang, bei dem überprüft wird, ob der Benutzer berechtigt ist, eine oder mehrere Aktionen mit dem Ausweis durchzuführen (auf eine oder mehrere Informationen zugreifen, Daten schreiben, Anwendungen oder Dateien erstellen oder löschen ...).

DHCP	Englisches Akronym für "Dynamic Host Configuration Protocol" (Protokoll zur dynamischen Host-Konfiguration). Ein Netzwerkprotokoll, dessen Aufgabe es ist, die IP-Parameter eines Netzwerkgeräts (PC, Server-Arbeitsplatz, Client-Arbeitsplatz ...) automatisch zu konfigurieren, indem ihm eine IP-Adresse, eine Subnetzmaske und ein Gateway zugewiesen werden.
DTMF	Englisches Akronym für Dual-Tone Multi-Frequency (SF für Stimmfrequenz auf Deutsch). Diese Technologie ermöglicht es, aus der Ferne mit einem Sprachserver zu kommunizieren und von einem Überwachungszentrum aus Befehle zu senden, die das Ansprechen aus der Ferne erlauben und/oder Abhörmikrofone aktivieren.
Einbruchsprofil	Eine Gruppe von Meldergruppen, auf die ein Operator Einbruch einwirken kann. Dieses Profil besteht aus bis zu drei Listen von Meldergruppen oder Melderinformationen: eine Basisgruppe, die die Ein-/Ausschaltung eines definierten Satzes von Gruppen ermöglicht, und zwei (Teil-)Untergruppen, die die teilweise Ein-/Ausschaltung der Anlage ermöglichen.
Empfänger	Bezeichnet beim Einbruchsmanagement die Entität, die für den Empfang von Alarmen ausgewählt wurde - in der Regel ein Fernüberwachungszentrum.
Gateway	**Kommunikations-Gateway**: eine optionale Lizenz, die erworben werden kann, um den MICROSESAME-Server mit Systemen Dritter zu verbinden (LDAP-Server, biometrisches System MORPHO MANAGER ...). **Import- oder Export-Gateway**: optionale Lizenzen, die die Nutzung von CSV-Dateien zum Abrufen (Importieren) oder Bereitstellen (Exportieren) einer Reihe von Informationen im Zusammenhang mit den Benutzer-IDs des Standorts nutzen.

	Netzwerk-Gateway: Netzwerkgerät, das IP-Pakete zwischen mehreren Geräten weiterleitet. Meistens handelt es sich dabei um Router.
ID-Mittel	Element, das den Zutritt eines Benutzers ermöglicht. ID-Mittel können verschiedene Technologien (Schlüsselanhänger, Karte, Nummernschild, Fingerabdruck, numerischer Code ...) und verschiedene Lesegeräte zum Auslesen verwenden.
IP	Englisches Akronym für Internet Protokoll. Das Internetprotokoll ermöglicht es den Geräten, die es verwenden, über TCP- oder UDP-Pakete miteinander zu kommunizieren. Das IP-Protokoll wird über drahtgebundene lokale Netzwerke transportiert, die das Ethernet-Verbindungsprotokoll verwenden. Netzwerkkarten oder Schnittstellen mit RJ45-Anschlüssen haben physischen Zutritt und werden logisch über ihre IP-Adresse identifiziert.
Kodierungstabelle	Eine Kodierungstabelle ist eine Tabelle, in der wir für jede Art von Alarm (Einbruch, Feuer, etc.) einen Ereigniscode definieren werden, der an die Fernüberwachung gesendet wird. Diese Codes sind daher mit dem gewählten Fernüberwachungsmonitor abzustimmen.
Kommunikationsprotokoll	Ein Satz von Regeln und Konventionen, der die Kommunikation und Interoperabilität zwischen verschiedenen Computersystemen ermöglicht. Das Protokoll definiert die Struktur der an den Empfänger gesandten Nachricht. Die folgenden Protokolle können zwischen dem TILLYS und einem Überwachungszentrum verwendet werden: ● CESA 200: jedes übertragene Ereignis besteht aus einem numerischen Code von 01 bis 96. ● ID-Contact: jedes Ereignis besteht aus zwei numerischen Codes, einem Typ- oder Kategorie-Code von 001 bis DDD und einem zweiten Ereigniscode für einen gegebenen Typ von 001 bis 999. Außerdem wird die Nummer des Users übermittelt, der eine Abteilung in Betrieb nimmt bzw. außer Betrieb nimmt.
Lesegerät	Ausrüstung, die zur Erkennung eines ID-Mittels in einem System zur Zutrittskontrolle verwendet wird. Das ID-Mittel kann verschiedene Formen annehmen: Ausweis, Tastaturcode,

	biometrischer Fingerabdruck, Nummernschild... Je nach Technologie kann ein Lesegerät verwendet werden, um: ● Sicherstellung der einfachen Erkennung des Trägers des ID-Mittels, z. B. ein Lesegerät vom Typ "transparent", das sich darauf beschränkt, das Vorhandensein eines Ausweises zu erkennen. ● Zusätzlich das Lesen eines Standard ID-Mittels sicherstellen, z. B. ein "einfaches" Lesegerät, das nur die Seriennummer eines Ausweises lesen kann (*CSN-ID*). ● Zusätzlich die Funktion des Entschlüsselns einer sicheren ID-Mittel gewährleisten, die in einem Ausweis codiert ist, z. B. ein sicheres Lesegerät, in dem der Schlüssel für die Ausweise gespeichert wird.
LVE	Akronym für Lokale Verarbeitungseinheit. IP-basierte Speicherprogrammierbare Steuerung, die in den Bereichen Zutrittskontrolle, Einbruch und Gebäudeautomatisierung eingesetzt wird. Diese Steuerung verwaltet z. B. den Zutritt von Usern, Informationen von Lesegeräten oder Einbruchschutzsystemen usw. Die LVE von TIL TECHNOLOGIES heißt die *TILLYS*.
Manueller Auswurf	Eine Maßnahme, mit der ein Benutzer die Überwachung trotz eines Fehlerzustands bei einem oder mehreren Meldern ermöglicht.
Melder	**Physischer Melder**: ein Gerät, dessen Aufgabe es ist, einen Einbruch in einem Bereich zu erkennen, und das verschiedene Arten von Sensoren verwendet: Magnetkontakt, Infrarotsensor, Mikrowellensensor... Ein Melder ist mit zwei Kontakten ausgestattet, die jeweils eine Information liefern: einen Alarmkontakt (*AL-Kontakt* , der eine Erfassungsinformation nennt) und einen Manipulationsschutzkontakt (*AP-Kontakt*, der eine Information über das Öffnen oder Herausziehen des Melders liefert). Bei TIL kann ein physischer Melder nur zu einer einzigen *Meldergruppe* gehören. **Virtueller Melder**: ein logischer Melder, der mithilfe von TILLYS-internen Registern definiert wird. In einer Installationskonfiguration, in der ein physischer Melder zu zwei Meldergruppen gehören soll, wird seine Funktion mit der eines virtuellen Melders verknüpft (z. B. durch Mikrocode). Der physische Melder wird dann in einer der Gruppen gemeldet und der dazugehörige virtuelle Melder in der anderen Gruppe.

Meldergruppe	Eine Gruppe von Meldern, die innerhalb desselben Gebäudes, derselben Etage, Abteilung oder Sonstigem durch eine operative logische Verknüpfung verbunden sind und einen gemeinsamen Modus für : ● das Ein- und Ausschalten der Überwachung, ● das Senden von Alarm-Codes an einen Fernüberwachungsmonitor, ● die Verwaltung einer oder mehrerer Sirenen, ● die Implementierung von Voralarmen oder Überschreibungsmechanismen. Pro Einbruchfunktion können bis zu 32 Gruppen deklariert werden.
Melderinformation	Informationen vom Typ ToR, die von einem physischen Melder (Radar, Türkontakt, Manipulationsschutzkontakt ...) oder einem virtuellen Register (internes Register der TILLYS) stammen.
Microcode	Eine spezielle Programmiersprache, die von TILLYS ausgeführt wird, um seine Funktionsweise angesichts von Ereignissen zu definieren, die ihm von allen Geräten, mit denen er verbunden ist, übermittelt werden.
MICROSESAME	Software zur einheitlichen Überwachung, mit der alle elektronischen Informationen des Gebäudes zentralisiert werden können: Zutrittskontrolle, Einbruchserkennung, technische Verwaltung, Video, Gegensprechanlage... Die Steuerung der verschiedenen Funktionen über eine gemeinsame Grafikschnittstelle macht deren Bedienung deutlich einfacher und die Eingriffe effizienter. Da die Interaktionen zwischen den verschiedenen Systemen vollständig automatisiert werden können (Aktionen auf Ereignisse), ist auch die Verarbeitungsgeschwindigkeit gewährleistet.
POE	Englisches Akronym für Power Over Ethernet. Netzwerkfunktionalität zur Bereitstellung von Strom über das Ethernet-Kabel.
Polling	Polling ist eine Funktion, die bei der Verwendung einer IP-Kommunikation genutzt wird. Sie ermöglicht es dem Fernüberwachungsmonitor, die IP-Übertragungsfunktion abzufragen, um sicherzustellen, dass die Verbindung zwischen beiden Geräten funktioniert.
Port	Einstiegspunkt zu einem Dienst (Web-Dienst, DNS-Dienst, Mail-Dienst...) auf einem Gerät (PC, Server...), das mit einem Netzwerk

	verbunden ist. Ports stellen eingehende oder ausgehende Zutritte dar und ermöglichen es, dass verschiedene Software und/oder Betriebssysteme miteinander kommunizieren können.
RS 485	In der Industrie verwendeter Kommunikationsstandard. Seine Umsetzung durch TIL TECHNOLOGIES ermöglicht es, Materialien in Bus- und/oder Sternform bis zu einer Entfernung von 600 Metern mit dem *TILLYS* zu verbinden.
Sirenenfunktion	TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Ihre Einstellungen wirken sich auf die verschiedenen Arten von Klingeltönen aus, die bei Ereignissen erzeugt werden, auf das Verhalten der Haupt- und Zusatzsirenenfunktion und deren Auslöseart sowie auf die Zuweisung der entsprechenden Meldergruppen.
Sperrung	Bezeichnet den deaktivierten Zustand eines Teils eines Einbruchschutzsystems, in dem das Auftreten einer Einbruch- oder Überfallalarmbedingung nicht an die Notrufzentrale gemeldet werden kann; dies gilt bis zur manuellen Aufhebung.
TACTILLYS	TIL TECHNOLOGIES Tastatur, die dem Management des Einbruchs V1 gewidmet ist und mit einem 7-Zoll-Farbbildschirm ausgestattet ist. Angeschlossen an einen RS 485-Bus der TILLYS, ermöglicht es einem Einbruchsmanagement-Operator, sich zu authentifizieren, um auf bestimmte Aktionen zuzugreifen, die in der Einbruchsfunktion parametriert sind. Sie kann mit einem Lesegerät für Ausweise ausgestattet sein, das den einzugebenden Code ersetzt oder im Gegenteil die notwendige Authentifizierung eines Einbruchsmanagement-Operator verstärkt (Vorbeiziehen eines Ausweises + Eingabe eines Codes).
Tastaturfunktion	TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Ihre Parametrierung wirkt sich auf die Verwaltung der betroffenen Meldergruppen und die Verwaltung des internen Summers der verschiedenen definierten Tastaturen aus.
TILLYS	Von TIL TECHNOLOGIES entwickelte *IP* speicherprogrammierbare Steuerung, die über Funktionen für Zutrittskontrolle, Einbruchserkennung und *Gebäudeleittechnik* verfügt. Über 3 RS 485-Busse (A, B und C) ermöglicht jeder TILLYS den Anschluss von 8, 16 oder 24 Lesegeräten für die Zutrittskontrolle. Er ist auch eine echte Alarmzentrale. Siehe auch *LVE*.
Übertragungsfunktion	TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Die TILLYS Einstellung wirkt sich auf die der Fernüberwachungsmonitore (die als "Empfänger" bezeichnet werden und maximal 4 sein dürfen), die genutzten Protokolle

	(CESA 200 oder ID Contact), die zu übertragenden Codes und die gewünschten Anrufprofile (gleichzeitige Anrufe oder Backups) aus. Die Übertragungsfunktion ermöglicht es außerdem, bis zu 32 Fernsteuerungen pro Einbruchsfunktion zu definieren, mit denen Operatoren der Fernüberwachung je nach zugewiesenem Niveau (2, 9 oder 32 Fernsteuerungen) Fernaktionen am Standort durchführen können.
User	Person, die über einen Zutritt zum Standort verfügen muss, der durch das System der Zutrittskontrolle geschützt ist. Ein User kann über eine oder mehrere mehrere ID-Mittel verfügen. Die User können sein: ● Personen, die ständig am Standort arbeiten (User vom Typ "Daueruser"), ● Personen, die außerhalb des Standorts tätig sind (User mit einer bestimmten Gültigkeitsdauer, die der Dauer ihrer Tätigkeit entspricht), ● Personen, die nur vorübergehend Zutritt zum Standort haben (User vom "Besucher"-Typ).
Verbindungsmodus	Einstellung des Modus auf dem MOBILIS-Terminal 3. Dieser kann entweder im Modus "Offline" betrieben werden, dann arbeitet er nach dem Importieren der Datenbank mit den ID-Mitteln vom MICROSESAME-Server im Standalone-Modus, oder im "Online"-Modus, dann ist er über eine WLAN-Verbindung mit dem MICROSESAME-Server verbunden.
Vereinfachte Inbetriebnahme	Bei Einbruch wird die Inbetriebnahme standardmäßig vorgeschlagen, wenn sich ein Benutzer an einer Einbruchstastatur anmeldet. Das vereinfachte Update zeigt drei verschiedene Meldergruppen an: Die erste enthält alle in der Einbruchfunktion definierten Gruppen, die zweite und dritte sind die sogenannten "Teilgruppen", die die gleichzeitige Inbetriebnahme von vorgewählten Gruppen ermöglichen.
Voralarm	Bei der Einbruchsfunktion definiert der Voralarm die Verzögerung zwischen einer Aufforderung zur Inbetriebnahme und dem tatsächlichen Start der Überwachung. Der Einsatz des Voralarms wird häufig implementiert, um mit Überschreibungen umgehen zu können. Der Voralarm erzeugt einen speziellen Klingelton, sobald er ausgelöst wird, und warnt potenzielle Bewohner vor der bevorstehenden Bereichsüberwachung, wobei ihnen die Möglichkeit gegeben wird, eine Überschreibung vorzunehmen.
WEBSESAME	Web-Anwendung der MICROSESAME-Software. Sie ermöglicht die Nutzung eines Großteils der Funktionen von MICROSESAME

	mithilfe eines einfachen Internetbrowsers (Edge, Chrome, Firefox, Safari...). Man spricht in diesem Fall von einem "leichten Client-Arbeitsplatz".
Zyklischer Test	Regelmäßiger Vorgang, der von der TILLYS durchgeführt wird und darin besteht, eine Übertragungsfunktion an einen Empfänger durchzuführen, um die Funktion der Kommunikationslinie zu überprüfen. Seine Periodizität ist einstellbar. Die Übertragung des zyklischen Tests kann zeitgesteuert oder zeitunabhängig sein oder an die Inbetriebnahme einer oder mehrerer Gruppen gekoppelt werden. Es ist möglich, einen zyklischen Test pro Empfänger einzustellen.

Kapitel 1. Hintergrund zur Erkennung von Einbrüchen

1.1. Überblick über die Basisversion von CUBE Einbruch

Die Hardware-Architektur ist von der Art, wie sie im folgenden Diagramm dargestellt ist.

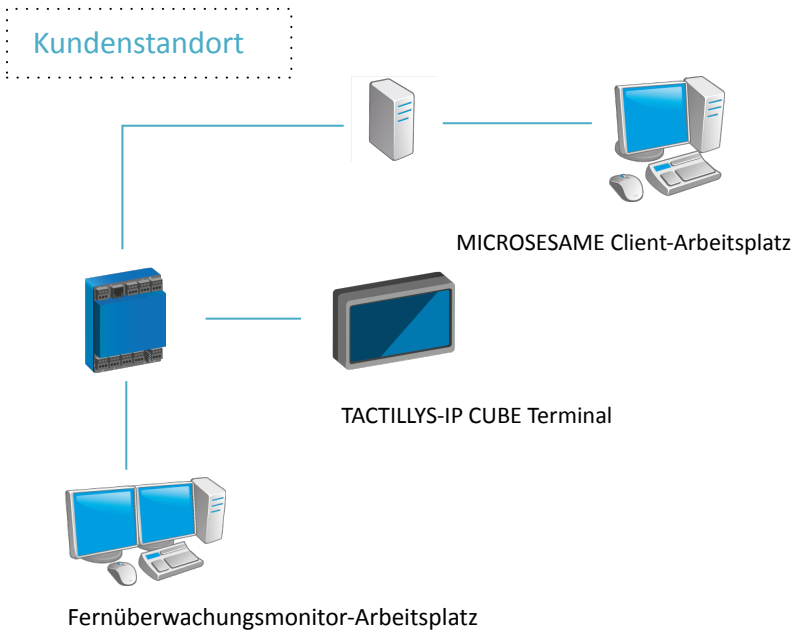

Abbildung 1.1. Hardware-Architektur der Basisversion von CUBE Einbruch (10010-001)

Die TILLYS, mit der das Terminal TACTILLYS-IP CUBE verbunden ist, verwaltet die Meldergruppe. Seine Melder und Sirenen sind überschaubar:

- über das Terminal TACTILLYS-IP CUBE,
- durch den Client-Arbeitsplatz MICROSESAME,
- über die Station des Fernüberwachungsmonitors.

1.2. Überblick über die Multi-TILLYS-Version des CUBE Einbruchs

Wenn es notwendig ist, Melder und Sirenen auf mehrere TILLYS zu verteilen, ist dies nun möglich, indem ein Host-TILLYS und ein oder mehrere Geräte-TILLYS verwendet werden, die über IP in einem Ethernet-Netzwerk verbunden sind.

Die Melder und Sirenen der Geräte-TILLYS sind dann virtuell mit der Meldergruppe des Host-TILLYS verbunden, der sie so verwaltet, als wären sie physisch mit ihm verbunden.

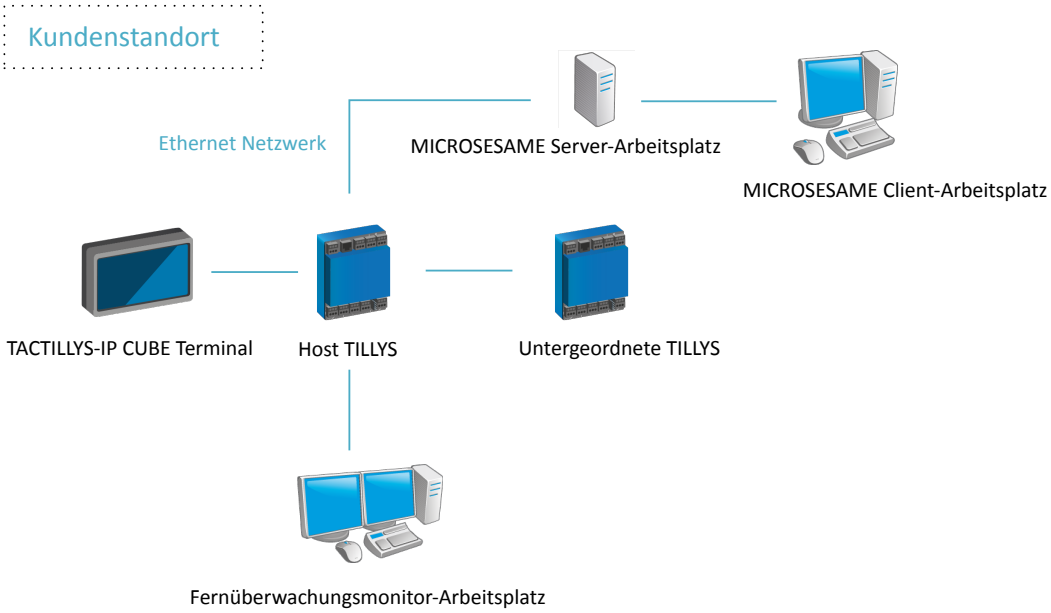

Abbildung 1.2. Hardware-Architektur der Multi-TILLYS-Version des CUBE Einbruchs (10010-002)

Die folgende Abbildung zeigt die physischen Verbindungen zwischen den Meldern und ihren TILLYS in einem Gebäude sowie die logischen Verbindungen über IP. Diese ermöglichen es, virtuelle Melder und Sirenen auf dem TILLYS-Host zu deklarieren sowie mit MICROSESAME und mit Fernüberwachungssystemen wie F1 zu kommunizieren.

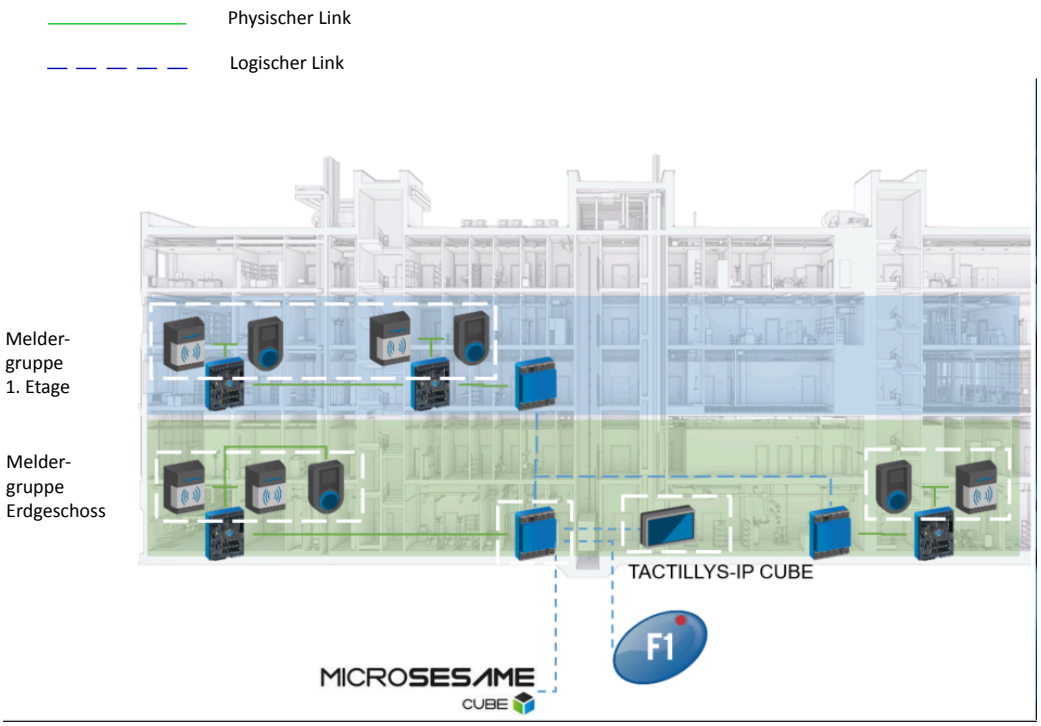

Abbildung 1.3. Multi-TILLYS-Konfiguration des Einbruchs CUBE (10010-003)

1.3. Neuheiten und Vorteile von CUBE Einbruch

Die CUBE Einbruch-Lösung bietet vier wichtige Neuerungen im Vergleich zur vorherigen Version:

- Die Verwendung von*IP* anstelle des RS 485-Busses zwischen dem Terminal TACTILLYS-IP CUBE und der *TILLYS*.
- Die Konfiguration wird an der *TILLYS* vorgenommen, bevor die Informationen in *MICROSESAME* hochgeladen werden.
- Die Logik Normal zu ist bei Meldern weit verbreitet.
- Die Inbetriebnahme ist ohne Eingabe einer Mikrocode-Linie möglich.

In funktionaler Hinsicht bietet der CUBE Einbruch vier entscheidende qualitative Vorteile gegenüber dem Marktangebot:

- Eine Cybersicherheit auf demselben Niveau wie die Zutrittskontrolle, die ANSSI-zertifiziert ist.
- Integration der Überwachung durch die Verwendung von Melderobjekten, Meldergruppen und Sirenen.
- Verbesserte ergonomische Nutzung durch native Überwachungsobjekte und Widgets, die in MICROSESAME animiert werden.

- Mehr Leistung bei den Fernüberwachungsfunktionen durch IP-Terminals für mehrere Zentralen und die Nutzung der SIA-Übertragung.

1.4. Definition der erwarteten Funktionsweise durch den Sicherheitsbeauftragten

Der Sicherheitsbeauftragte legt die erwartete Funktionsweise fest, in einem **Lastenheft** oder einer **Funktionsbeschreibung**.

Dieses Dokument und der **Netzwerk-Adressierungsplan** ermöglichen es dem TIL TECHNOLOGIES-Partner, die Bereiche der Zutrittskontrolle und die Gruppen der Einbruchserkennung in seinen Räumlichkeiten zu definieren, bevor er sie am Standort seines Kunden einsetzt.

1.5. CUBE Einbruch-Voraussetzungen, die vom CISO des Kunden zu implementieren sind

Da die Übertragung der Einbruch-Daten über ein IP-Netzwerk erfolgt, gelten die folgenden Standards.

Titel des Standards	Verweis und Link
SIA Digital Communication Standard - Internet Protocol Event reporting	[*SIA-DC-09*]
Security Communications - Digital Communications Standard - "SIA Format" Protokoll - for Alarm System Communications (Kommunikation über Alarmsysteme)	[*SIA-DC-03*]
SIA Digital Communications Standard - Receiver-to-Computer Schnittstelle Protocol - for Central Station Equipment Communications (Standard für die Kommunikation zwischen Receivern und Computern)	[*SIA-DC-07*]

Tabelle 1.1. Geltende Standards für Computersicherheit

1.6. Management von Einbrüchen CUBE

Dieser Abschnitt enthält eine große Tabelle mit möglichen Operationen, die vom Status des Einbruchschutzsystems abhängen.

Alarm-Status	Was und wie?	Warum?	Wo und von wem?
Vor dem Scharfmachen	Einrichten von Gruppen Zutrittsverzug Austrittsverzug Automatischer Auswurf Automatische Wiedereinführung Dauerhafter Auswurf	Bestimmen Sie, was auf der Ebene des Managements von Einbrüchen getan werden kann und wer berechtigt ist, diese Operationen durchzuführen.	TILLYS Gastgeber (Sicherheitsbeauftragter)
Im Voralarm	Überschreiben einer Meldergruppe	Erlaubt einem oder mehreren Mitarbeitern, nach der Endzeit in einem bestimmten Bereich für eine aus einer Liste von Werten auszuwählende Dauer weiterzuarbeiten. Auswurf einer fehlerhaften Gruppe.	TACTILLYS-IP CUBE Terminal (Benutzer mit Rechten Einbruch)
In Abweichung davon	Den Alarm scharf stellen	Beenden Sie die Überschreibung und schalten Sie den Alarm scharf.	TACTILLYS-IP CUBE Terminal (Benutzer mit Rechten Einbruch)
Im Voralarm	*Manueller Auswurf* eines fehlerhaften Melders	Erlauben Sie die Bewaffnung der Gruppe. Vermeiden Sie es, den Alarm durch Verlassen des Gebäudes vor Ablauf des Austrittsverzugs auszulösen.	TACTILLYS-IP CUBE Terminal (Benutzer mit Rechten Einbruch)

Alarm-Status	Was und wie?	Warum?	Wo und von wem?
Auf dem Austrittpfad	Verlassen Sie die Räumlichkeiten so schnell wie möglich	Vermeiden Sie es, den Alarm durch Verlassen des Gebäudes vor Ablauf des Austrittsverzugs auszulösen.	TACTILLYS-IP CUBE Terminal (Benutzer mit Rechten Einbruch)
Alarm scharf	Ausweis an der Tür	Erreichen des Terminals TACTILLYS-IP CUBE während des Zutrittsverzugs	Lesegerät für Zutrittskontrolle (Benutzer mit Einbruch-Rechten)
Auf dem Zutrittpfad	Ausweis auf dem TACTILLYS-IP CUBE und den Alarm entschärfen	Betreten der Räumlichkeiten außerhalb der Arbeitszeiten	TACTILLYS-IP CUBE Terminal (Benutzer mit Rechten Einbruch)
Alarm unscharf	Ausweis, um das Gebäude zu betreten Ändern bestimmter Einstellungen	Zugang zu den Räumlichkeiten während der Arbeitszeit Die Konfiguration zum Schutz vor Einbrüchen an die Bedürfnisse anpassen	Lesegeräte für die Zutrittskontrolle TILLYS Gastgeber (Sicherheitsbeauftragter)

Tabelle 1.2. Liste der Operationen zur Bewältigung von Einbrüchen mit ihrem Kontext und Modus

1.7. Hintergrundinformationen für Integratoren

1.7.1. Formate der zwischen TILLYS und Fernüberwachungsendgeräten ausgetauschten Frames

Dieser Teil mit seinen drei Abschnitten liefert **Integratoren** eine Referenzdokumentation aus den Normen SIA DC-09 und SIA DC-03 sowie Beispiele für ihre Umsetzung durch TIL TECHNOLOGIES.

Die TILLYS überträgt Frames im SIA-Format DC-09, die Nutzlasten im SIA-Format DC-03 transportieren. Da dieses Format interpretierbar ist, werden die SIA DC-03-Codes, die von der TILLYS an die Fernüberwachungsmonitore übertragen werden, sowie die Fernsteuerungen, die von den Fernüberwachungsmonitoren an die TILLYS gesendet werden, in den folgenden drei Abschnitten detailliert beschrieben.

1.7.1.1. Von Meldern an Fernüberwachungsmonitore gesendete Einbruch-Codes

Damit Einbruch-Codes für einen Melder **übertragen** werden, muss der Schalter **Alarme übertragen** im Abschnitt **Allgemeine Informationen** für diesen Melder aktiviert sein (siehe *Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“*).

Die folgende Tabelle enthält eine Liste der mit den Meldern verknüpften Einbruch-Codes.

Art des Signals	Erscheinen des Alarms	Verschwinden des Alarms	Sperrung	Enthemmung	Auswurf	Neueinspritzung
Einbruch	BA	BR	BB	BU	XW	BU
24/24	TA	TR	TB	TU	VW	TU
Lautloser Einbruch	BA	BR	BB	BU	XW	BU
Systemfehler	IA	IR	UB	UU	XW	UU
Lautloser Systemfehler	IA	IR	UB	UU	XW	UU
Notfall	QA	QR	QB	QU	XW	QU
Brand	FA	FR	FB	FU	XW	FU

Tabelle 1.3. Vollständige Liste der von den Meldern gesendeten Einbruch-Codes

Die folgende Tabelle gibt die Bedeutung dieser Codes zunächst in englischer und dann in französischer Sprache wieder.

Tastaturcode	Kurzbeschreibung	Lange Beschreibung	Übersetzung
BA	Burglary Alarm	Burglary zone has been violated while armed	Einbruch oder stilles Eindringen in einen scharfgeschalteten einbruchhemmenden Bereich
BR	Burglary Restoral	Alarm/ Störungszustand wurde beseitigt	Verschwinden des Alarm- oder Fehlerzustands
BB	Burglary Bypass	Burglary Bereich wurde umgangen	Das Signal für Einbruch oder stilles Eindringen in einen Bereich wurde gehemmt.

Tastaturcode	Kurzbeschreibung	Lange Beschreibung	Übersetzung
BU	Burglary Unbypass	Bereich Bypass wurde entfernt	Deaktivierung oder Wiedereinführung eines Bereichs für Einbruch oder stilles Eindringen
FA	Feuer Alarm	Fire condition detected	Auftreten eines Alarms vom Typ Feuer
FR	Fire Restoral	Alarm/ Störungszustand wurde beseitigt	Verschwinden des Alarms oder der Störung vom Typ Feuer
FB	Fire Bypass	Bereich wurde umgangen	Der Feueralarm, der in einem Bereich aufgetreten ist, wurde unterdrückt.
FU	Fire Unbypass	Bypass wurde entfernt	Deaktivierung eines Feueralarms in einem Bereich oder Rücksetzung dieses Bereichs
IA	Equipment Failure Condition	Ein spezifischer, übertragbarer Zustand wird an einem Gerät erkannt.	Alarm aufgrund eines Systemfehlers oder eines stillen Systemfehlers
IR	Equipment Fail - Restoral	The equipment condition has been restored to normal	Alarm verschwindet, wenn ein Systemfehler oder ein stiller Systemfehler vorliegt.
UB	Untypisierter Bereich Bypass	Bereich unbekannten Typs wurde umgangen	Sperrung des Signals vom Typ Systemfehler oder stiller Systemfehler
UU	Untyped Bereich Unbypass	Bypass wurde entfernt	Deaktivierung oder Neueingabe des Signals vom Typ Systemfehler oder stiller Systemfehler
QA	Emergency Alarm	Emergency assistance request	Alarm bei Notfallsignal erscheint

Tastaturcode	Kurzbeschreibung	Lange Beschreibung	Übersetzung
QR	Emergency Restoral	Alarm/ Störungszustand wurde beseitigt	Verschwinden von Alarmen bei Notfallsignalen
QB	Emergency Bypass	Bereich wurde umgangen	Sperrung des Notrufsignals in einem Bereich
QU	Emergency Unbypass	Bypass wurde entfernt	Deaktivierung oder Neueingabe des Notrufsignals in einem Bereich
TA	Tamper Alarm	Alarm equipment enclosure opened	Offener Alarmschutzkasten (Alarm erscheint bei einem 24/24-Signal)
TR	Restoral Tamper	Alarm Ausrüstungsgehäuse wurde geschlossen	Geschlossener Alarmschutzkasten (Alarm verschwindet bei 24/24-Signal)
TB	Tamper Bypass	Tamper detection has been bypassed	Die Erkennung des Manipulationsschutzes wurde gehemmt (Alarmhemmung bei Signaltyp 24/24).
TU	Tamper Unbypass	Tamper detection bypass has been removed	Die Erkennung des Manipulationsschutzes wurde deaktiviert (Disinhibition oder 24/24-Signalrückführung).
XW	Forced Point	Ein Punkt wurde zur gleichen Zeit aus dem System gezwungen.	Ein Punkt wurde beim Scharfschalten gewaltsam aus dem System ausgeworfen (Auswurf des Signals, unabhängig von der Art des Signals).

Tabelle 1.4. Bedeutung der von den Meldern gesendeten Einbruch-Codes

Der im Adressfeld (address field) übertragene Wert ist der Wert der Signalnummer des Melders.

1.7.1.2. Ereigniscodes, die von den Gruppen an die Fernüberwachungsmonitore übermittelt werden

Damit Ereigniscodes für eine Gruppe **übertragen** werden, muss der Schalter **Scharf-/ Unscharfschalten übertragen** im Abschnitt **Allgemeine Informationen** für diese Meldergruppe aktiviert sein (siehe *Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“*).

Die folgende Tabelle listet und beschreibt die Liste der gruppenbezogenen Ereigniscodes.

Tastaturcode	Kurzbeschreibung	Übersetzte lange Beschreibung	Ergänzende Informationen
ZK	Automatic Closing	Automatische Scharfschaltung des Systems	Bereich oder Punkt
OA	Automatic opening	Automatische Entschärfung des Systems	Bereich oder Punkt
CI	Fail to close	Automatische Scharfschaltung fehlgeschlagen	Nummer des Bereichs
CE	Closing Extend	Überschreiben, um die Bewaffnung abzuwehren	Nutzernummer

Tabelle 1.5. Bedeutung der von den Gruppen gesendeten Ereigniscodes

Der Wert, der im Adressfeld (address field) übertragen wird, ist der der Gruppennummer.

1.7.1.3. Fernsteuerungen, die von Fernüberwachungsmonitoren an TILLYS gesendet werden

Es können die in der folgenden Tabelle aufgeführten Fernsteuerungen verwendet werden.

Tastaturcode	Kurzbeschreibung	Weitere Informationen	Bedeutung
SA	Set Area	x*y set area x to y, (3 = User Defined, 2 = Perimeter Only, A = Armed, 0 = Disarmed)	Befehl zum Scharf- oder Unscharfschalten eines Bereichs

Tastaturcode	Kurzbeschreibung	Weitere Informationen	Bedeutung
SB	Set Bypass	x*y set bypass on Bereich x to y (1 = ON, O = OFF)	Befehl zur Sperrung oder Deaktivierung einer Gruppe
SS	Set Sounder	x*y set sounder x to y (1 = ON, O = OFF)	Befehl zum Stoppen oder Auslösen einer Sirene
TP	Trap Account	Konto, das für die Fernprogrammierung verwendet wird	Befehl zum Ändern des Wertes eines benutzerdefinierten Registers "custom TIL".

Tabelle 1.6. Liste der Fernsteuerungen, die von Fernüberwachungsmonitoren an TILLYS gesendet werden können

Für jede Fernsteuerung müssen Sie die Gruppennummer für die Scharfschaltung und die damit verbundene Verzögerung beim Scharf- und Unscharfschalten (sofort oder mit Voralarm), die Meldersignalnummer für den Muting-Befehl, die Sirenennummer für die Sirenenabschaltung, das Register und dessen Wert für die Fernsteuerung TP usw. angeben.

1.7.2. Werte des numerischen Registers für den Gruppenstatus bei Einbruch CUBE

Diese Informationen richten sich an **Integratoren**.

Das numerische Register für den Status von Gruppen wird durch das Attribut regStatus des group-Tags definiert. Jedes Bit in diesem Register entspricht einer Information gemäß der folgenden Tabelle.

Bit-Index	Hexadezimal-Maske	Beschreibung	Kommentar
0	0x1	1 = mindestens ein Fehler vom Typ "Alarm Einbruch" in der Gruppe 0 = kein Fehler vom Typ "Alarm Einbruch" in der Gruppe	Entspricht dem synthetischen Register ToR, das für den Typ "Alarm Einbruch" festgelegt werden kann.
1	0x2	1 = mindestens ein Fehler vom Typ "Alarm 24/24" in der Gruppe	Entspricht dem synthetischen Register ToR, das für den Typ "Alarm 24/24" festgelegt werden kann.

Bit-Index	Hexadezimal-Maske	Beschreibung	Kommentar
		0 = kein Fehler vom Typ "Alarm 24/24" in der Gruppe	
2	0x4	1 = mindestens ein Fehler vom Typ "Stiller Einbruch Alarm" in der Gruppe 0 = kein Fehler vom Typ "Stiller Einbruch Alarm" in der Gruppe	Entspricht dem synthetischen Register ToR, das für den Typ "Stiller Einbruch Alarm" festgelegt werden kann.
3	0x8	1 = mindestens ein Fehler vom Typ "Systemfehler" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe	Fehler im Logischen Register ToR Synthese, der für den Typ "Systemfehler" festgelegt werden kann.
4	0x10	1 = mindestens ein Fehler vom Typ "Notruf" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe	Entspricht dem synthetischen Register ToR, das für den Typ "Notruf" festgelegt werden kann.
5	0x20	1 = mindestens ein Fehler vom Typ "Systemfehler" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe	Entspricht dem zusammenfassenden Register ToR, das für den Typ "Feuer" festgelegt werden kann.
6	0x40	1 = mindestens ein Fehler vom Typ "Systemfehler leise" in der Gruppe 0 = kein Fehler des Typs "Leiser Systemfehler" in der Gruppe	Synthetischer ToR Register-Ausfall, der für den Typ "Stiller Systemfehler" festgelegt werden kann.
16	0x10000	1 = Gruppe bewaffnet 0 = Gruppe entschärft	
17	0x20000	1 = mindestens ein Alarm, der auf eine Quittierung wartet 0 = kein Alarm, der auf eine Quittierung wartet	

Bit-Index	Hexadezimal-Maske	Beschreibung	Kommentar
18	0x40000	1 = Voralarm läuft 0 = kein Voralarm im Gange	
19	0x80000	1 = Abweichung läuft 0 = keine Überschreibung im Gange	
20	0x100000	1 = Austrittsverzug läuft 0 = kein Austrittsverzug läuft	
21	0x200000	1 = Zutrittsverzug läuft 0 = kein Zutrittsverzug läuft	

Tabelle 1.7. Mögliche Werte des numerischen Registers für den Gruppenstatus

1.7.3. Register des Mikrocodes, spezifisch für den Einbruch CUBE

Die folgenden Register wurden zur Verwendung in MICROSESAME erstellt (siehe *TILLYS Mikrocode-Programmierhandbuch* - GP-100006-DE).

Zur Definition von physischen Meldern werden zwei neue Register verwendet: AL_DETECTEUR_ID und AP_DETECTEUR_ID.

Außerdem wurden zwei Virtuelle Register erstellt: ENTRE_AL_DETECTEUR_ID und ENTRE_AP_DETECTEUR_ID.

Schließlich werden neue Arten von Registern verwendet, um den Auswurf von Meldern zu verwalten: EJ_DETEKTOR_ID.

1.7.4. Befehl für den Mikrocode, spezifisch für den TACTILLYS-IP CUBE

Der Befehl GET_AP_TACTILLYS wurde erstellt, um die Informationen über den Manipulationsschutz des TACTILLYS-IP CUBE in MICROSESAME zurückzusenden.

Kapitel 2. CUBE Einbruch-Workflows

Dieses Kapitel bietet Geschäftsprozesse nach Benutzerprofilen (Partner, Installateur oder Startseite-Agent).

Sonstige Kapitel enthalten Anweisungen für :

- an den Sicherheitsbeauftragten (siehe *Kapitel 6, Sicherheitsmanagement durch den Sicherheitsbeauftragten*),
- Personen, die zur Benutzung des Terminals TACTILLYS-IP CUBE befähigt sind (siehe *Abschnitt 4.3, „Verwendung des TACTILLYS-IP CUBE“*),
- an Entwickler von Fernüberwachungssystemen von Drittanbietern (siehe *Abschnitt 1.7.1, „Formate der zwischen TILLYS und Fernüberwachungsendgeräten ausgetauschten Frames“*).

2.1. Vorbereitung des Standorts für den Computer

Wenn es sich um die erste Inbetriebnahme handelt, lesen Sie bitte die *Kurzanleitung (GD-10001-DE)*.

2.2. CUBE Einbruch-Konfiguration durch den Partner mit Vorbereitung in seinen Räumlichkeiten

2.2.1. Workflow - Vorkonfiguration Einbruch CUBE durch den Partner in seinen Räumlichkeiten

Die Partnerin führt vor ihrem Besuch beim Kunden in ihren Geschäftsräumen folgende Tätigkeiten aus:

1. Physische Verbindung des Laptops mit dem Ethernet-Netzwerk
2. *Abschnitt 3.2.1.1, „Zutritt zur Schnittstelle für den Administrator des CUBE Einbruchs auf einem TILLYS“*
3. *Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“*
4. *Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“*
5. *Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“*
6. *Abschnitt 3.2.2.1, „Erstellen von Einbruchsprofilen auf der Host-TILLYS“*
7. *Abschnitt 3.2.1.10, „Zuordnung eines TACTILLYS-IP CUBE-Terminals zu einer oder mehreren Gruppen einer Host-TILLYS“*
8. *Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“*
9. Weiter mit den Schritten von *Abschnitt 2.2.2, „Workflow - Exportieren/Importieren der CUBE Einbruch Einstellungen“*: Exportieren der Konfiguration, die der Partner in seinen Räumlichkeiten erstellt hat, und Importieren dieser Konfiguration auf den Standort des Kunden.

2.2.2. Workflow - Exportieren/Importieren der CUBE Einbruch Einstellungen

Diese beiden Prozesse ermöglichen :

- eine CUBE Einbruch-Konfiguration im Voraus vorzubereiten,
- eine CUBE Einbruch-Konfiguration zu speichern, um sie auf einen anderen TILLYS zu kopieren,
- eine CUBE Einbruch-Konfiguration auf den Standort eines Kunden zu kopieren,
- die Konfiguration eines TILLYS wiederherzustellen, um eine gespeicherte CUBE Einbruch-Konfiguration wiederherzustellen oder wenn dieser TILLYS ersetzt wird.

Um eine Einbruch-Konfiguration zu exportieren oder zu speichern :

1. *Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“*
2. *Abschnitt 3.2.4.2, „Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei“*

So importieren Sie eine gesicherte Einbruch-Konfiguration oder stellen sie wieder her :

1. *Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“*
2. *Abschnitt 3.2.4.2, „Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei“*
3. Weiter auf dem Standort des Kunden mit dem *Abschnitt 2.3.1, „Workflow - CUBE Einbruch-Konfiguration auf dem Standort des Kunden “*

2.3. Konfiguration Einbruch CUBE durch den Partner auf dem Standort des Kunden

2.3.1. Workflow - CUBE Einbruch-Konfiguration auf dem Standort des Kunden

Der Partner führt direkt in der Kundschaft die folgenden Operationen durch:

1. Physische Verbindung des Laptops mit dem Ethernet-Netzwerk
2. *Abschnitt 3.2.1.1, „Zutritt zur Schnittstelle für den Administrator des CUBE Einbruchs auf einem TILLYS“*
3. *Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“*
4. *Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“*
5. *Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“*
6. *Abschnitt 3.2.2.1, „Erstellen von Einbruchsprofilen auf der Host-TILLYS“*
7. *Abschnitt 3.2.1.10, „Zuordnung eines TACTILLYS-IP CUBE-Terminals zu einer oder mehreren Gruppen einer Host-TILLYS“*
8. *Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“*
9. Weiter mit *Abschnitt 2.3.2, „Workflow - Konfigurieren eines Ausweises für den Zutritt zum Terminal TACTILLYS-IP CUBE“*

2.3.2. Workflow - Konfigurieren eines Ausweises für den Zutritt zum Terminal TACTILLYS-IP CUBE

Die Startseite kann Ausweise für den Zutritt mit Einbruch-Rechten vorbereiten.

1. *Abschnitt 5.2.1, „Vorbereitung eines Ausweises zur Kontrolle gegen Einbrüche“*
2. *Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »*
3. *Section 5.2.3, « Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer »*
4. *Section 5.2.4, « Zuweisung von Zutritten an einen neuen Benutzer »*
5. *Section 5.2.5, « Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen »*
6. Weiter mit *Abschnitt 2.3.3, „Workflow - Installation, Konfiguration und Parametrierung eines TACTILLYS-IP CUBE-Terminals vor seiner Inbetriebnahme“*

2.3.3. Workflow - Installation, Konfiguration und Parametrierung eines TACTILLYS-IP CUBE-Terminals vor seiner Inbetriebnahme

Bei der ersten Inbetriebnahme muss der Partner oder der Installateur nacheinander die folgenden Schritte durchführen:

1. *Abschnitt 4.1.1, „Physische Installation und Verbindung eines TACTILLYS-IP CUBE-Terminals“*
2. *Abschnitt 4.1.2, „Zutritt zur Schnittstelle für den Administrator des TACTILLYS-IP CUBE-Terminals und Anzeige der Produktmerkmale“*
3. *Abschnitt 4.2.2, „Abfrage der Betriebsmerkmale von TACTILLYS-IP CUBE“*
4. *Abschnitt 4.2.3, „Parametrierung des TACTILLYS-IP CUBE“*
5. *Abschnitt 4.1.3, „Änderung des Passworts für den Administrator des TACTILLYS-IP CUBE-Terminals“*
6. *Abschnitt 4.1.6, „Aktualisierung der Firmware des TACTILLYS-IP CUBE“*
7. *Abschnitt 4.1.4, „Einstellen der Uhrzeit des Terminals TACTILLYS-IP CUBE“*
8. *Abschnitt 4.1.5, „Netzwerk-Einstellungen des TACTILLYS-IP CUBE“*
9. *Abschnitt 5.1, „Importieren der CUBE Einbruch-Konfiguration in MICROSESAME“*

Kapitel 3. Parametrisierung des CUBE Einbruchs durch den Partner

Mit dem Einbruch CUBE wird nun fast die gesamte Parametrisierung auf der TILLYS-Ebene durchgeführt. Dies ermöglicht es den Partnern, die Konfiguration der TILLYS im Voraus vorzubereiten, um sie dann vor Ort schnell zu laden, bevor sie den oder die TACTILLYS-IP CUBE-Terminals installieren. Alle diese Vorgänge können bereits vor der Installation von MICROSESAME durchgeführt werden und einsatzbereit sein.

3.1. Hardware-Architektur für die Konfiguration des CUBE Einbruchs durch den Partner

Der Partner kann die Konfiguration bei seinem Endkunden durchführen, aber er kann auch eine CUBE Einbruch-Konfiguration in seinen eigenen Räumlichkeiten vorbereiten, bevor er sich auf den Weg macht, um sie am Standort des Kunden zu implementieren. Die erforderliche Hardware-Architektur besteht einfach aus :

- Von einem Laptop, der mit Ethernet verbunden ist,
- Ein oder mehrere TILLYS (Multi-TILLYS-Konfiguration), die mit demselben Ethernet-Netzwerk verbunden sind.

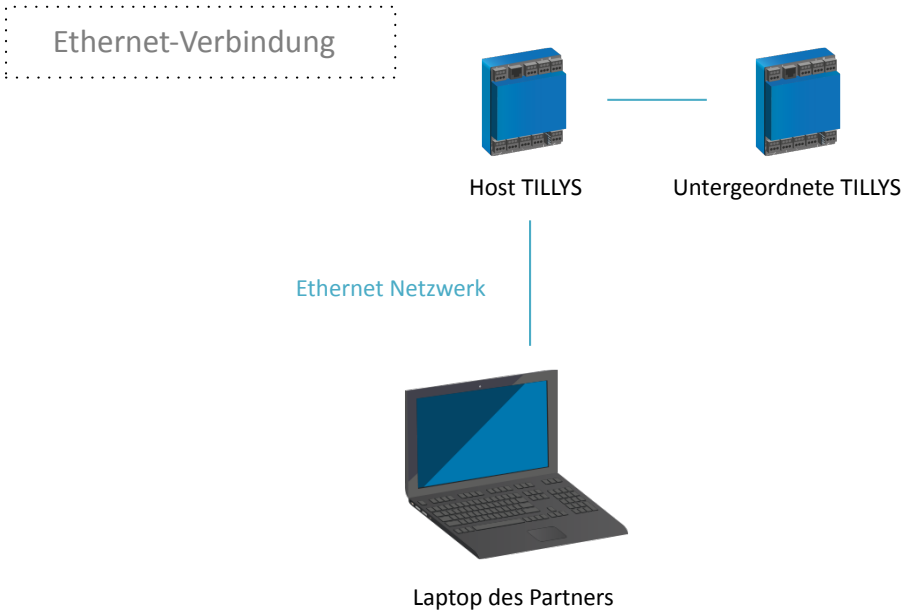

Abbildung 3.1. Einrichten von CUBE Einbruch über Ethernet (10010-004)

3.2. Konfiguration, Parametrierung und Wartung des CUBE Einbruchs auf der TILLYS

Die Konfiguration der Einbruchmeldeanlage (die anschließend auf den/die TILLYS heruntergeladen werden muss) kann auf jedem TILLYS vor der Konfiguration der Anlage beim Kunden durchgeführt werden.

Wenn Melder und Sirenen in einer Entfernung angeschlossen werden müssen, die über die zulässige Gesamtlänge desRS 485-Busses (600 Meter) hinausgeht, ermöglicht der CUBE Einbruch die Einrichtung von TILLYS-Geräten. Der TILLYS Host verwaltet dann die Einbruch-Konfiguration für die Melder und Sirenen der TILLYS Geräte, die mit ihm verbunden sind, und ein Token sichert den Informationsaustausch.

3.2.1. Konfigurationsoperationen Einbruch CUBE

In den folgenden Abschnitten werden alle individuellen Konfigurationsvorgänge aufgeführt, die über die webbasierte Schnittstelle eines TILLYS über dessen IP-Adresse zugänglich sind.

3.2.1.1. Zutritt zur Schnittstelle für den Administrator des CUBE Einbruchs auf einem TILLYS

1. Öffnen Sie auf dem Laptop, der mit dem Ethernet-Netzwerk verbunden ist, einen Browser und geben Sie die IP-Adresse des TILLYS ein, den Sie konfigurieren möchten.
2. Geben Sie den Login und das Passwort für den Zutritt ein.
3. Folgen Sie im Menü ☰ burger den Schritten **Einbruch CUBE > Einbruch Configuration**.
   Die Konfigurationsregisterkarten (Gruppen, Melder, Sirenen, Profile und TACTILLYS-IP) sind oben im Zentralenabschnitt zugänglich: siehe (1) in der folgenden Abbildung.

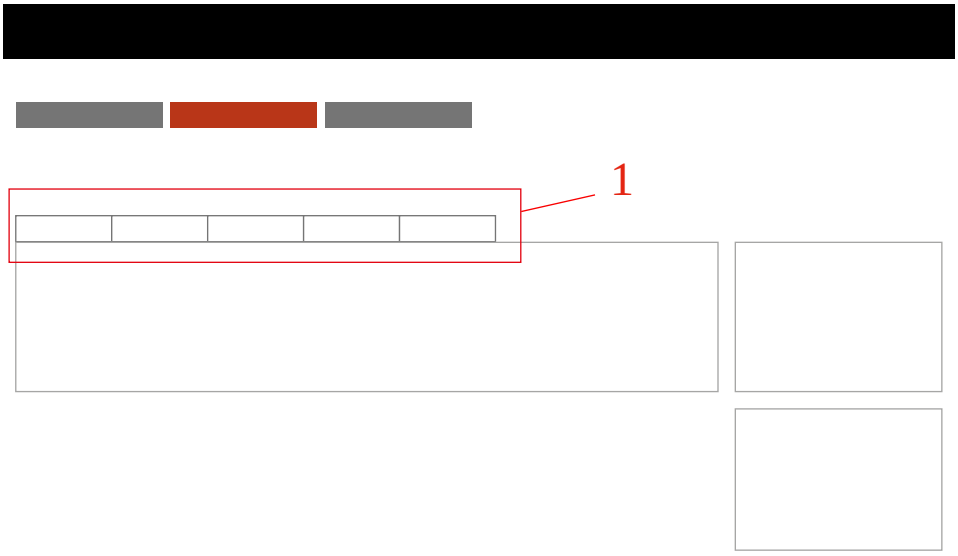

Abbildung 3.2. Position der Navigationsregisterkarten auf dem Konfigurationsbildschirm für den CUBE Einbruch eines TILLYS (10010-005)

3.2.1.2. Einrichten einer Gruppe von CUBE Meldern für den Einbruch

Mit Einbruch CUBE kann eine Meldergruppe der Host-TILLYS Melder und Sirenen verwalten, die physisch an verschiedene TILLYS angeschlossen sind (Multi-TILLYS-Konfiguration). Jeder TILLYS kann bis zu 32 Meldergruppen verwalten. Jede Gruppe kann physische Melder und virtuelle Melder verwalten, die mit anderen Sonstigen TILLYS verbunden sind.

Es ist völlig unnötig, eine Meldergruppe auf den TILLYS-Geräten zu erstellen. Mit dem CUBE Einbruch können sie ihre Melder und Sirenen virtuell mit der Meldergruppe des TILLYS-Hosts verknüpfen.

1. Folgen Sie im Menü ☰ burger auf dem TILLYS-Host **Einbruch CUBE > Einbruch Configuration**.
2. Klicken Sie auf den Reiter **Gruppen** und dann auf die Schaltfläche **[+ Hinzufügen]**.

3. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Detail der Einstellungen
Bezeichnung	Geben Sie einen repräsentativen Namen des Standorts für die Meldergruppe ein.
Übertragen die Scharfschaltung / Unscharfschaltung	Wenn die Scharf-/ Unscharfschaltungsaktionen der Gruppe an den Fernüberwachungsmonitor übertragen werden sollen, klicken Sie auf den Schalter (weiß > blau).
Register des Rüstungsstatus	Geben Sie unbedingt ein Register ToR (M, V oder R, von 1 bis 128) ein, das die Gruppe scharf (Wert 0) oder unscharf (Wert 1) schaltet.
Register für den Status (Statusregister)	Geben Sie optional ein numerisches Register (MN, VN oder RN, von 1 bis 128) ein, in das der gesamte Status der Gruppe hochgeladen wird. Siehe auch *Abschnitt 1.7.2, „Werte des numerischen Registers für den Gruppenstatus bei Einbruch CUBE“*.

Abschnitt Konfiguration der Bewaffnung	Detail der Einstellungen
Zeitplan für die automatische Scharfschaltung	Wenn eine automatische Scharfschaltung nach Zeitfenster gewünscht wird, geben Sie die Nummer eines Zeitfensters ein (von 1 bis 250).
Automatische Unscharfschaltung	Wenn die Gruppe am Ende eines Zeitfensters entschärft werden soll, klicken Sie im Rahmen der Zeitfensterentschärfung auf den Schalter (weiß > blau).
Register der Scharfschaltungsbereitschaft	Gibt an, ob die Meldergruppe scharfgeschaltet werden kann: ● Das Register ist 1, wenn keines der Meldersignale in der Gruppe im Fehlerzustand ist. ● Das Register wird auf 0 gesetzt, wenn mindestens ein Meldersignal in der Gruppe im Fehlerzustand ist.

Abschnitt Konfiguration der Bewaffnung	Detail der Einstellungen
	Geben Sie ggf. ein ToR-Register ein (M, V oder R, von 1 bis 128). Wenn das Signal eines Melders, der als **bei der Scharfschaltung automatisch auswerfbar** definiert ist, im Fehlerzustand ist, ist der Wert des Registers für den *Scharfschaltungsstatus* 0. Wenn die Scharfschaltung angefordert wird (automatisch, per *Mikrocode* oder per Fernsteuerung durch einen Operator), wird der Melder aus der Überwachungsschleife ausgeworfen und die Gruppe scharfgeschaltet.
Voralarm-Verzögerung (in Minuten)	Ermöglicht das Einstellen einer Verzögerung, bevor die Scharfschaltung der Gruppe ausgelöst wird. Geben Sie die gewünschte Anzahl von Minuten ein.
Zutrittsverzug (in Sekunden)	Geben Sie die gewünschte Anzahl von Sekunden ein, wenn mindestens ein Melder in der Gruppe als Zutrittsverzug konfiguriert wurde. Diese Verzögerung gilt für alle Melder in der Gruppe, die auf "Zutrittsverzug" oder "Ausgeblendet, wenn Zutrittszeit läuft" eingestellt sind.
Austrittsverzug (in Sekunden)	Geben Sie die gewünschte Anzahl von Sekunden ein, wenn mindestens ein Melder in der Gruppe als Austrittsverzug konfiguriert wurde. Diese Verzögerung gilt für alle Melder in der Gruppe, die auf "Austrittsverzug" oder "Ausgeblendet, wenn Eingangstempo läuft" eingestellt sind.
Mindestüberschreibung (in Minuten)	Legt den Mindestwert für die vorgeschlagene Überschreibungszeit beim Scharfschalten fest.

Abschnitt Konfiguration der Bewaffnung	Detail der Einstellungen
	Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.
Maximale Überschreibung (in Minuten)	Ermöglicht die Einstellung des maximalen Wertes für die Zeit, die für das Überschreiben der Scharfschaltung benötigt wird. Nach Ablauf dieser Zeit muss der Operator entscheiden, ob er die Gruppe entwaffnen oder die Bewaffnung zulassen will. Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.
Keine Überschreibung (in Minuten)	Legt den Schritt fest, um den die Zeit für das Überschreiben der Scharfschaltung erhöht wird. Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.

Abschnitt Zusammenfassende Register	Detail der Einstellungen
Es ist möglich, den Speicherort von 7 zusammenfassenden Registern festzulegen.	Sie ermöglichen es, ein Register für jeden Alarmtyp zu definieren, das das Vorhandensein eines Fehlerzustands in mindestens einem Signal eines Melders der Gruppe : ● Das Register wird auf 0 gesetzt, wenn keines der Meldersignale in der Gruppe im Fehlerzustand ist. ● Das Register wird auf 1 gesetzt, wenn mindestens ein Meldersignal in der Gruppe im Fehlerzustand ist. Geben Sie optional ein Register ToR (M, V oder R, von 1 bis 128) für jeden Alarmtyp ein : Einbruch, Rund um die Uhr, Stiller Einbruch, Systemfehler, Stiller Systemfehler, Notruf oder Brand.

4. Klicken Sie zur Validierung auf die Schaltfläche **[Speichern]**.

3.2.1.3. Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät

Der Anschluss der Melder und Sirenen der TILLYS Geräte muss unter Verwendung eines Tokens (Wertmarke) pro TILLYS Gerät erfolgen. Dies ermöglicht es, im Falle eines Sicherheitsproblems jedes TILLYS Gerät unabhängig voneinander zu trennen.

Token werden nur einmal generiert und müssen in einer Kundendatei zusammen mit seinen anderen vertraulichen Konfigurationsdaten aufbewahrt werden.

1. Folgen Sie im Menü  burger auf dem TILLYS-Host **Netzwerk und Sicherheit > Sicherheit**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

HTTPS-Abschnitt	Detail des Parameters
Select Zertifikat	Im Prinzip gibt es in diesem Abschnitt nichts zu ändern.

Abschnitt API-Tokens	Detail der Einstellungen
Token name (Name des Tokens)	Geben Sie einen Namen ein, der den entfernten TILLYS eindeutig identifiziert. Aus Sicherheitsgründen werden Sonderzeichen nicht berücksichtigt.
Days of validity (Tage der Gültigkeit) (Ablaufdatum)	Maximal 3 Jahre (d. h. 1096 Tage).
Scopes (Betreff)	Klicken Sie auf den Schalter **Tillys Konfiguration** (weiß > blau).

3. Klicken Sie zur Validierung auf die Schaltfläche **[Request New Token]**. Ein Fenster **Sicherheit** wird angezeigt.
4. Ganz rechts auf der Linie, die für die Eingabe des Passworts vorgesehen ist, befindet sich eine Schaltfläche zum Anzeigen des Passworts und die nächste zum Kopieren des Passworts.

   Kopieren Sie den Wert dieses Tokens in die Konfigurationsdatei der Client-Installation und notieren Sie dort auch die IP-Adresse des TILLYS-Geräts, für das es generiert wurde.
5. Um eine Unterbrechung der CUBE-Einbruchüberwachung in bestimmten Bereichen, in denen das Token abgelaufen ist, zu vermeiden, legen Sie bereits jetzt mit dem Kunden den Termin für den technischen Besuch zur Verlängerung der Gültigkeitsdauer des Token oder der Token fest (z. B. eine Woche vor dem geplanten Ablaufdatum).

3.2.1.4. Multi-TILLYS-Konfiguration: Kopie der Verbindung mit dem Host-TILLYS auf ein Gerät-TILLYS

Dieser Vorgang ermöglicht es, die Meldergruppe(n) des Host-TILLYS auf einem Geräte-TILLYS anzuzeigen.

Wenn es mehrere TILLYS-Geräte gibt, ist es ratsam, ein Token pro TILLYS-Gerät zu setzen (siehe *Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät“*).

1. Folgen Sie im Menü ☰ burger des TILLYS Geräts **Einbruch CUBE > Einbruch Configuration** und klicken Sie dann auf die Registerkarte **Groups**.
2. Klicken Sie auf der rechten Seite des Bildschirms auf die Schaltfläche **[Gruppen von einem Remote-Host herunterladen]**.

   Ein Dialogfenster wird angezeigt.

Abbildung 3.3. Eingeben des Token des Host-TILLYS auf einem Gerät-TILLYS (10010-010)

3. Füllen Sie die verschiedenen Felder gemäß der folgenden Tabelle aus.

Parameter	Details
Der abgesetzte Host verwendet HTTPS	In der Standardkonfiguration ist dieser Schalter aktiviert (weiß > blau) und das Protokoll https muss bei beiden TILLYS aktiviert sein. Ist dies nicht der Fall, wird die Nachricht "Hostgruppen konnten nicht gezogen werden: Host nicht erreichbar" angezeigt. Weitere Informationen finden Sie unter *Abschnitt 3.2.2.6, „Wahl der Sicherheitsstufe über IP zwischen TILLYS und TACTILLYS-IP CUBE“*.
Host	Standardmäßig enthält dieses Feld den Wert "admin". Geben Sie die IP-Adresse des TILLYS-Hosts ein.

Parameter	Details
API-Schlüssel	Fügen Sie den Wert des zuvor erzeugten Tokens ein (siehe *Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät“*).

4. Klicken Sie auf die Schaltfläche **[Gruppen herunterladen]**.

3.2.1.5. Konfiguration der CUBE Einbruchmelder einer TILLYS

Dies gilt für die TILLYS (Host oder Gerät), mit der die Melder physisch verbunden sind.

1. Gehen Sie im Menü  burger der TILLYS auf **Einbruch CUBE > Einbruch Configuration**, klicken Sie auf die Registerkarte **Melder** und dann auf die Schaltfläche **[+ Hinzufügen]**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Details zu den Einstellungen
Bezeichnung	Geben Sie einen Namen für den Melder ein.
Weiterleiten von Alarmen	Klicken Sie auf den Schalter (weiß > blau), wenn die von diesem Melder erzeugten Alarme an den Fernüberwachungsmonitor weitergeleitet werden sollen.
Blockierregister	Geben Sie optional ein Register ToR (M, V oder R, von 1 bis 128) ein, das im Zustand 1 die Sperrung des Melders ermöglicht (z. B. für Wartungsarbeiten).
Virtueller Melder	Standardmäßig ist der eingestellte Melder ein physischer Melder (der Schalter *Virtueller Melder* ist weiß). Geben Sie den *Bus* (A, B oder C), die Adresse des MI-Moduls, an das der Melder angeschlossen ist, und den ML-Eingang, mit dem er verdrahtet ist, ein. Einen virtuellen Melder zu konfigurieren bedeutet, ihn logisch mit einem TILLYS-Host zu verknüpfen, während er physisch mit einem TILLYS-Gerät verbunden ist. Dazu betätigen Sie den Schalter *Virtual Detector* (weiß > blau). Die Nummer dieses virtuellen Melders wird dann automatisch festgelegt (ID in der globalen Melderliste vorhanden).

Abschnitt Auswurf	Details der Einstellung
	Um die gewünschte Auswurfart für den Melder zu wählen, aktivieren Sie die Schalter (weiß > blau) : ● *Kann manuell ausgeworfen werden*: Manueller *Auswurf* bei der Inbetriebnahme ● *Kann automatisch ausgeworfen werden*: Automatischer *Auswurf* bei Inbetriebnahme ● *Kann dauerhaft ausgeworfen werden*: Dauerbenutzer *Auswurf* ● *Kann automatisch zurückgesetzt werden*: Automatische Rücksetzung nach Fehlerbehebung
Abschnitt Pfad Zutritt	**Details der Einstellung**
	Um einem Benutzer zu erlauben, nach dem Scharfschalten den Raum zu verlassen oder zum Unscharfschalten zum Einbruchsterminal zu gehen, und um die gewünschte Verzögerungsart zu wählen, aktivieren Sie die Schalter (weiß > blau). Die Verzögerungszeiten in Sekunden müssen in den Einstellungen der Meldergruppen konfiguriert werden. ● Aktiviert *den Zutrittsverzug*: Aktiviert den Zutrittsverzug. ● *Auf dem Eingangspfad*: Ausgeblendet, wenn der Zutrittsverzug läuft. Der Melder wird vorübergehend gehemmt, wenn ein anderer Melder in der gleichen Meldergruppe einen Zutrittsverzug oder Austrittsverzug hat. ● *Auf dem Weg zum Ausgang: Austrittsverzug*
Abschnitt Signale	**Details der Einstellung**
	Standardmäßig sind beide Signale, Alarm und Manipulationsschutz, aktiviert

Abschnitt Signale	Details der Einstellung
	(blauer Schalter). Um eines der Signale zu deaktivieren, klicken Sie auf seinen Schalter (blau > weiß). Der Alarm Einbruch kann ausgelöst werden, wenn die Gruppe scharfgeschaltet ist. Eine Sirenenfunktion wird ausgelöst, wenn sie verknüpft wurde. Der Manipulationsschutz-Alarm ist ein Dauerbenutzer-Alarm, der unabhängig vom Scharfschaltungsstatus der Gruppe ausgelöst wird. Eine Sirenenfunktion wird ausgelöst, wenn sie verknüpft wurde. ● *Alarm* : Anklicken, um ihn zu aktivieren (weiß > blau). *Typ* (Art des Alarms): Standardmäßig Einbruch. Wählen Sie den gewünschten Typ aus dem Drop-Down-Menü aus. *Modus*(Kontaktart): Wählen Sie einen Wert aus der Drop-Down-Menüleiste aus*(Normal zu*). *Nummer für den Fernüberwachungsmonitor* : Wert, der an den Fernüberwachungsmonitor übermittelt werden soll. ● *Selbstschutz*: Anklicken, um ihn zu aktivieren (weiß > blau). *Typ* (Art des Alarms): Standard 24/24. Wählen Sie den gewünschten Typ aus dem Drop-Down-Menü aus. *Modus* (Kontaktart) : *Normal zu*. *Nummer für den Fernüberwachungsmonitor* (Fernübertragungsreferenz): Wert, der an den Fernüberwachungsmonitor übermittelt werden soll.

Abschnitt Der Gruppe zuweisen	Details der Einstellung
	Um den Melder einer Gruppe zuzuweisen, wählen Sie seinen Namen aus der Drop-Down-Menüliste.

Abschnitt Der Gruppe zuweisen	Details der Einstellung
	Wenn es sich um einen virtuellen Melder handelt, muss er einer Gruppe des TILLYS-Hosts zugeordnet werden. Mit diesem Drop-Down-Menü können Sie auch einen Melder deaktivieren.

3. Um die vorgenommenen Einstellungen zu validieren, klicken Sie auf die Schaltfläche **[Speichern]**.

3.2.1.6. Einrichten eines CUBE-Einbruchmelders auf einem TILLYS-Gerät

In einer Multi-TILLYS-Konfiguration ist das Verfahren bis zur Auswahl der Anschlussgruppe identisch mit dem in *Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“* beschriebenen Verfahren: Wählen Sie die Hauptgruppe, die sich auf der Host-TILLYS befindet. Außerdem muss der Schalter *Virtueller Melder* aktiviert werden.

3.2.1.7. Einrichten einer CUBE Einbruch-Sirene

Dies gilt für die TILLYS (Host oder Gerät), mit der die Sirene physisch verbunden ist.

Jeder Klingelton-Stil hat einen Prioritätsindex. Je höher dieser Prioritätsindex ist, desto höher ist die Priorität des Klingeltons gegenüber den anderen.

Beispiele: Der Alarmton für Einbruch (Priorität 4) hat Vorrang vor dem Alarmton für Voralarm (Priorität 1), und der Alarmton für Feuer (Priorität 6) hat Vorrang vor dem Alarmton für Einbruch (Priorität 4).

1. Gehen Sie im Menü  burger der TILLYS auf **Einbruch CUBE > Einbruchskonfiguration**, klicken Sie auf die Registerkarte **Sirenen** und dann auf die Schaltfläche **[+ Hinzufügen]**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Detail der Einstellungen
Bezeichnung	Geben Sie einen Namen für die Sirene ein.
Befehlsregister	Geben Sie einen gültigen Wert für das Logische Register : Sei ein physisches Register für die Ausgabe eines Moduls, z. B. : "XA0102". Bei einem MLIO16-Modul müssen die Ausgänge zuvor definiert worden sein, damit das Register akzeptiert wird. Oder ein virtuelles Register: Ein Register des Typs M, V oder R von 1 bis 128 kann eingegeben werden, um einen bestimmten,

Abschnitt Allgemeine Informationen	Detail der Einstellungen
	vom Mikrocode definierten Trigger auszulösen.
Blockierregister	Geben Sie optional einen Wert für das Logische Register (M, V oder R, von 1 bis 128) ein, der auf 1 gesetzt wird, um die Sperrung der Sirene zu ermöglichen (z. B. für Wartungsarbeiten).

Abschnitt Sirenen-Stile	Detail der Einstellungen
Voralarm	Konfigurieren Sie die verschiedenen Sirenen mithilfe der Zeichen + und - sowie die Dauer des Klingelns (in Sekunden). Die Konfiguration der Sirenen erfolgt auf der Ebene der Dauer und nicht auf der Ebene der Anzahl der Wiederholungen. Bei der Sirene für den Voralarm, Auslösung vor der Scharfschaltperiode, damit die Person, die die Gruppe scharfgeschaltet hat, das Gebäude verlassen kann oder eine noch anwesende Person am Terminal TACTILLYS-IP CUBE eine Überschreibung beantragen kann.
Scharfstellung	Auslösung zu Beginn der Scharfschaltung der Gruppe.
Systemfehler	Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe.
Einbruch	Auslösung bei Erkennung eines Einbrechers, wenn die Gruppe scharfgeschaltet ist.
Notfall	Notruf. Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe.
Brand	Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe.

Abschnitt Gruppen zuweisen	Detail der Einstellungen
	Mithilfe dieser Liste können Sie eine Sirene einer oder mehreren Gruppen zuweisen. Um mehrere Gruppen auszuwählen, halten Sie die **[CTRL]-** Taste gedrückt und klicken Sie

Abschnitt Gruppen zuweisen	Detail der Einstellungen
	nacheinander auf die Gruppen, dann lassen Sie die **[CTRL]**-Taste los.

3. Um die vorgenommenen Einstellungen zu validieren, klicken Sie auf die Schaltfläche **[Speichern]**.

3.2.1.8. Konfigurieren einer CUBE Einbruch-Sirene auf einem TILLYS Gerät

In der Konfiguration Einbruch CUBE multi-TILLYS ist das Verfahren identisch mit dem unter *Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“* beschriebenen, bis zur Auswahl der Anschlussgruppe: Wählen Sie die Hauptgruppe, die sich auf dem Host-TILLYS befindet.

3.2.1.9. Übersichtsvergleich der Melder für Einbruch CUBE multi-TILLYS

Die Kombination der Taste **[Windows]** auf der Tastatur mit der linken **[←]** oder rechten **[→]** Pfeiltaste ermöglicht es, ein Browserfenster in Pfeilrichtung um die Hälfte zu verkleinern und zwei Fenster auf demselben Bildschirm nebeneinander zu legen, um ihre Informationen leichter vergleichen zu können.

1. Öffne ein Browserfenster und öffne den TILLYS-Host, dann klicke auf die Tasten **[Windows]** + **[←]**.
   Das Browserfenster wird in der Breite verkleinert und nimmt die linke Hälfte des Bildschirms ein.
2. Gehen Sie im Menü ☰ burger des TILLYS-Hosts auf **Einbruch CUBE > Einbruch Configuration** und klicken Sie auf die Registerkarte **Melder**.
3. Öffnen Sie ein zweites Browserfenster und öffnen Sie das TILLYS Gerät, klicken Sie dann auf die Tasten **[Windows]** + **[→]**.
   Das Browserfenster wird in der Breite verkleinert und nimmt die rechte Hälfte des Bildschirms ein.
4. Im Menü ☰ burger des TILLYS Geräts folgen Sie **Einbruch CUBE > Einbruch Configuration** und klicken Sie auf die Registerkarte **Detektoren**.
   Durch den Vergleich der beiden Konfigurationen auf einem Bildschirm lassen sich mögliche Fehlkonfigurationen erkennen.

3.2.1.10. Zuordnung eines TACTILLYS-IP CUBE-Terminals zu einer oder mehreren Gruppen einer Host-TILLYS

Diese Operation ermöglicht es, ein TACTILLYS-IP CUBE Terminal mit der Host-TILLYS zu verbinden, dessen Gruppe(n) Sensoren, Sirenen sowie alle mit dem Scharf- und Unscharfschalten des Alarms verbundenen Operationen verwaltet/verwalten.

1. Im Menü ☰ burger des TILLYS-Hosts folgen Sie **Einbruch CUBE > Configuration Einbruch**, klicken Sie auf die Registerkarte **TACTILLYS-IP** und dann auf die Schaltfläche **[+ Hinzufügen]**.

2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Detail der Einstellungen
Bezeichnung	Geben Sie einen Namen für das TACTILLYS-IP CUBE-Terminal ein.
IP-Adresse	Geben Sie die IP-Adresse dieses TACTILLYS-IP CUBE-Terminals ein.
Port	Geben Sie den Kommunikationsport ein, der für die Nutzung der Kommunikation mit dem Terminal verwendet wird (Standard: 443).
Alarme weiterleiten	Klicken Sie auf den Schalter (weiß > blau), damit das Terminal einen Signalton abgibt, wenn im System ein Alarm erzeugt wird.

Abschnitt Authentifizierung	Detail der Einstellungen
Maximale Inaktivität (in Sekunden)	Geben Sie die gewünschte Anzahl an Sekunden ein, die der Zeitspanne entspricht, in der das Terminal ohne jegliche Aktion des Operators verbunden bleibt.
Maximale Anzahl an Versuchen vor dem Sperren	Geben Sie die Anzahl der Verbindungsversuche ein, die akzeptiert werden, bevor das Terminal gesperrt wird.
Dauer der Authentifizierungssperre	Geben Sie die Zeit in Minuten ein, für die das Terminal gesperrt bleibt, nachdem die maximale Anzahl an Verbindungsversuchen erreicht wurde.
Zeitlimit für die Eingabe des Codes (in Sekunden)	Geben Sie die maximale Zeit in Sekunden ein, die zwischen dem Passieren eines Ausweises und der Eingabe des zugehörigen Codes akzeptiert wird.
Willkürliche Position der Tasten auf der numerischen Tastatur	Klicken Sie auf den Schalter (weiß > blau), um die Zufallspositionierung der numerischen Tasten zu aktivieren.

Abschnitt Signale	Detail der Einstellungen
Manipulationsschutz	Klicken Sie auf den Schalter (weiß > blau), um die Berücksichtigung des Selbstschutzsignals des Terminals zu aktivieren.

Abschnitt Signale	Detail der Einstellungen
Typ	Wenn aktiviert, ist der Manipulationsschutz standardmäßig auf den Alarmtyp 24/24 eingestellt. Wählen Sie eventuell einen anderen Alarm-Typ aus dem Drop-Down-Menü aus.
Nummer für den Fernsender	

Abschnitt Verwaltete Gruppen	Detail des Parameters
Der Gruppe zuweisen	Mit dieser Liste können Sie ein TACTILLYS-IP CUBE-Terminal der Verwaltung einer oder mehrerer Gruppen zuweisen. Um mehrere Gruppen auszuwählen, halten Sie die **[CTRL]-** Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die **[CTRL]-**Taste los.

3. Klicken Sie zur Validierung auf die Schaltfläche **[Speichern]**.

3.2.1.11. Konfigurieren von Fernüberwachungsmonitoren

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Transmitter-Konfiguration** und klicken Sie dann auf die Schaltfläche **[+ Hinzufügen]**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Detail der Einstellungen
Abschnitt **Allgemeine Informationen**	
Bezeichnung	Geben Sie einen Namen für den Fernüberwachungsmonitor ein.
IP-Adresse	Geben Sie die IP-Adresse des Fernüberwachungsmonitors ein.
Port	Geben Sie den Kommunikationsport des Fernüberwachungsmonitors ein.

Abschnitt Einstellungen des Empfängers	Detail der Einstellungen
Protokoll	SIA-DCS.
Abonnentennummer	Geben Sie die vom Fernsender bereitgestellte Kundenreferenz ein.

Abschnitt Einstellungen des Empfängers	Detail der Einstellungen
Anzahl der Verbindungsversuche	Geben Sie die maximale Anzahl an Verbindungsversuchen ein.
Zeit zwischen den Versuchen (in Sekunden)	Geben Sie die Mindestzeit zwischen zwei Verbindungsversuchen ein.

Abschnitt Einstellungen für den zyklischen Test des Empfängers	Detail der Einstellungen
Startzeit	Die Frames des zyklischen Tests werden von der TILLYS an die Überwachungssoftware des Fernüberwachungsmonitors (SIG) gesendet. Es gibt einen zyklischen Test pro Fernüberwachungsmonitor. Mit dieser Einstellung können Sie die Referenzzeit festlegen, ab der der zyklische Test durchgeführt wird.
Intervall (in Minuten)	Mit diesem Parameter können Sie festlegen, wie oft der zyklische Test durchgeführt werden soll.

Abschnitt Polling-Einstellungen des Empfängers	Detail des Parameters
Der Gruppe zuweisen	*Polling-Frames* werden von der Host-TILLYS an das Frontend der Fernüberwachung gesendet. Diese Liste ermöglicht es Ihnen, ein TACTILLYS-IP CUBE-Terminal einer oder mehreren Gruppen zuzuordnen. Um mehrere Gruppen auszuwählen, halten Sie die **[CTRL]**- Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die **[CTRL]**-Taste los.

Abschnitt Notrufempfänger	Detail des Parameters
Zum Beispiel "Fernüberwachungsmonitor 2".	Um aus diesem Drop-Down-Menü einen Rettungsempfänger auswählen zu können, muss dieser zunächst eingerichtet werden.

3. Klicken Sie zur Validierung auf die Schaltfläche **[Speichern]**.

4. Um einen Fernüberwachungsmonitor zu erstellen, beginnen Sie wieder bei Schritt 1, um diesen neuen Empfänger zu erstellen, bearbeiten Sie dann den Hauptempfänger und weisen Sie ihm im letzten Abschnitt des Eingabebildschirms den neu erstellten Notrufempfänger zu.

3.2.1.12. Anzeige der Fernüberwachungskonfiguration

Im Menü burger des TILLYS-Hosts folgen Sie **Einbruch CUBE > Senderkonfiguration** und klicken Sie dann auf die Schaltfläche **[Aktuelle Konfiguration]**.

3.2.2. Parametrisierung und Wartung des CUBE Einbruchs

In den folgenden Abschnitten werden die Einstellungsvorgänge für die CUBE Einbruchfunktion erläutert, z. B. die Detailtiefe der Protokollierungsfunktion, die Sicherheitsstufe für den Austausch über IP und die Verwendung des spezifischen Mikrocodes für die CUBE Einbruchfunktion.

Sie stellen auch die Wartung vor, wie z. B. das Löschen der Schlüssel, bevor ein defektes TACTILLYS IP-Terminal zum Kundendienst geschickt wird, sowie die Maßnahmen zur Sicherung und Wiederherstellung einer Konfiguration.

3.2.2.1. Erstellen von Einbruchsprofilen auf der Host-TILLYS

1. Folgen Sie im Menü burger des TILLYS-Hosts **Einbruch CUBE > Einbruch Configuration**, klicken Sie auf die Registerkarte **Profile** und dann auf die Schaltfläche **[+ Hinzufügen]**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

Abschnitt Allgemeine Informationen	Detail des Parameters
Bezeichnung	Geben Sie einen Namen für das Benutzerprofil Einbruch CUBE ein.

Abschnitt Rechte des Profils	Detail des Parameters
Sieben Schalter (1 pro Zutritt)	Klicken Sie auf den Schalter (weiß > blau), um das entsprechende Recht zu aktivieren.

Abschnitt Verwaltete Gruppen	Detail des Parameters
Drop-Down-Menü	Diese Liste ermöglicht es Ihnen, ein TACTILLYS-IP CUBE-Terminal einer oder mehreren Gruppen zuzuordnen. Um mehrere Gruppen auszuwählen, halten Sie die **[CTRL]-** Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die **[CTRL]-**Taste los.

3. Klicken Sie zur Validierung auf die Schaltfläche **[Speichern]**.

4. Füge alle benötigten Profile hinzu, indem du die oben genannten Schritte wiederholst.

3.2.2.2. Auswahl der Meldergruppen, die von einem TACTILLYS-IP CUBE verwaltet werden

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.
2. Markieren Sie im ersten Abschnitt auf der linken Seite des Bildschirms das Kontrollkästchen der Gruppe.
3. Wählen Sie im ersten Abschnitt auf der rechten Seite des Bildschirms die Gruppe(n), die mit dem TACTILLYS-IP CUBE verbunden ist/sind, und klicken Sie auf die Schaltfläche **[Zuweisen]**.

3.2.2.3. Auswahl des Modus für die Authentifizierung (Ausweis oder Ausweis + Code) an einem TACTILLYS-IP CUBE

Informationen zum Einstellen oder Ändern des personalisierten Tastaturcodes eines Benutzers finden Sie unter *Abschnitt 6.2, „Änderung des ID-Mittels Einbruch, das bei der Ausweis- und Code-Identifikation auf TACTILLYS-IP CUBE verwendet wird.“*.

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.
2. Klicken Sie im zweiten Abschnitt auf der rechten Seite des Bildschirms auf das Drop-Down-Menü Modus für die Authentifizierung. Wählen Sie *Ausweis* oder *Ausweis & personalisierter Tastaturcode und* klicken Sie dann auf die Schaltfläche **[Authentifizierungseinstellungen anwenden].**

3.2.2.4. Auswahl der Applets, die auf einen TACTILLYS-IP CUBE geladen werden sollen

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.
2. Geben Sie im dritten Abschnitt auf der rechten Seite des Bildschirms eine Indexreferenz ein, klicken Sie auf die Schaltfläche **[Durchsuchen]**, wählen Sie die Datei aus **,** die **Sie** herunterladen möchten, validieren Sie und klicken Sie auf die Schaltfläche **[Applet-Einstellungen anwenden].**

3.2.2.5. Auswahl der Detailebene für Ereignisse im TILLYS-Protokoll

Die Protokollierung von Ereignissen hilft dabei, die Ursache von Fehlfunktionen zu finden. Sie kann in einer Datei gespeichert oder im Laufe der Zeit an einen Computer gesendet werden, auf dem Syslog Watcher installiert ist.

Die laufende Anzeige der Protokollierung ermöglicht es, die Logs in Echtzeit zu verfolgen. Es ist möglich, beide Optionen zu aktivieren (in einer Datei speichern und im Ereignisticker anzeigen)...

Je höher die Detailtiefe, desto mehr Rechenleistung verbraucht der Prozessor und desto mehr Speicherplatz wird belegt. Dies kann die Leistung verlangsamen.

1. Im Menü ☰ burger des TILLYS-Hosts folgen Sie **System > Logs**.
2. Um das Protokoll an eine bestimmte IP-Adresse zu senden, geben Sie diese IP-Adresse und den Zielport (standardmäßig 514) ein, klicken Sie auf den Syslog-Schalter (grau > blau) und klicken Sie dann auf die Schaltfläche **[Submit]**.

   Um das Protokoll in einer Datei zu speichern, klicken Sie auf den Syslog-Schalter (grau > blau) und dann auf die Schaltfläche **[Submit]**.

   Um das Protokoll direkt in der Debug-Konsole am unteren Rand dieses Bildschirms anzusehen, klicken Sie auf den Weblog-Schalter (grau > blau) und dann auf die Schaltfläche **[Submit]**.

   Es ist möglich, alle drei Schalter zu aktivieren.
3. Klicken Sie auf die grauen Schaltflächen, um auszuwählen, bei welchen Aspekten ein hoher Detaillierungsgrad erforderlich ist.

   Es ist möglich, eine niedrigere Detailstufe wiederherzustellen, indem Sie auf die blauen Schaltflächen **[Normal]** klicken.

   Zur Validierung klicken Sie auf die Schaltfläche **[Submit]**.
4. Eine Debugging-Konsole mit Filtern und einem Bereich für die Suche ermöglicht es, die Suche zu verfeinern.

3.2.2.6. Wahl der Sicherheitsstufe über IP zwischen TILLYS und TACTILLYS-IP CUBE

Mit dieser Option können Sie die Sicherheitsstufe für den Austausch zwischen TACTILLYS-IP und TILLYS auswählen (Protokoll http oder https). Standardmäßig ist der Modus https, was ein sicherer Modus ist. Es wird nicht empfohlen, den Modus http zu verwenden.

1. Klicken Sie in der Schnittstelle für den Administrator des TACTILLYS-IP auf das Symbol ☰ burger in der oberen linken Ecke und folgen Sie **Configuration > Security**.
2. Wählen Sie im Drop-Down-Menü **Select a certificate** den **Eintrag None** und klicken Sie auf die Schaltfläche **[Submit]**.
3. Auf der TILLYS-Ebene muss die gleiche Einstellung im Bildschirm **Netzwerkkonfiguration** vorgenommen werden: Folgen Sie **Netzwerk und Sicherheit > Netzwerkkonfiguration**.
4. Scrollen Sie nach unten, deaktivieren Sie die Option **Sichere Kommunikation** (Wechsel von blau zu grau) und klicken Sie auf die Schaltfläche **[Speichern].**
5. Falls erforderlich, wird die Wiederherstellung der Kommunikation im Modus https in denselben Bildschirmen durchgeführt.

3.2.2.7. Löschen der TACTILLYS-IP-Schlüssel (Desetzen)

Diese Möglichkeit sollte genutzt werden, nachdem ein TACTILLYS-IP aus einer Anlage entfernt wurde, um ihn in eine andere Anlage integrieren zu können, oder bevor er zum Kundendienst geschickt wird.

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Erase Keys**.
2. Klicken Sie auf die Schaltfläche **[Erase Keys]**.

3.2.3. Operationen zur Bewältigung von Einbrüchen

3.2.3.1. Auswurf oder Wiedereinwurf eines Melders

Alle diese Schritte werden auf dem Einstellungsbildschirm jedes Melders durchgeführt.

1. Von der Schnittstelle für Administratoren des TACTILLYS-IP CUBE aus klicken Sie auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Einbruch Cube > TILLYS-Konfiguration**.
2. Klicken Sie auf die Registerkarte Melder.
3. Klicken Sie auf der Linie des Melders, den Sie auswerfen oder neu einfügen möchten, auf die Schaltfläche **[Bearbeiten]**.
4. Klicken Sie im Abschnitt Auswurf auf den Schalter der Option, die Sie aktivieren möchten (weiß > blau).
5. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche **[Speichern].**

3.2.4. Wartung von Einbruch CUBE

3.2.4.1. Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS

1. Von der Schnittstelle zum Administrator eines TILLYS aus klicken Sie auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Netzwerk und Sicherheit > Netzwerk-Tools.**
2. Klicken Sie auf die Schaltfläche **[Service-Port** aktivieren **]**, um ihn zu aktivieren (blau) oder zu deaktivieren (weiß).
3. Klicken Sie auf **[Speichern].**

3.2.4.2. Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei

1. Um eine CUBE Einbruch-Konfigurationsdatei auf einem TILLYS exportieren oder importieren zu können, muss dessen Wartungsport aktiviert sein (siehe *Abschnitt 3.2.4.1, „Aktivieren*

oder Deaktivieren des Ports für die Wartung eines TILLYS"). Ist dies nicht der Fall, ist die Option Importieren/Exportieren nicht einmal im Menü sichtbar.

2. Von der Schnittstelle für den Administrator des TILLYS-Hosts aus klicken Sie auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **General > Import/Export Configuration**.
3. Füllen Sie die verschiedenen Felder gemäß der folgenden Tabelle aus.

Parameter	Details
Abschnitt **Importieren von Konfigurationen**	Um eine Konfigurationsdatei zu importieren, klicken Sie auf die Schaltfläche **[Browse]**, wählen Sie eine Datei aus, klicken Sie auf die Schaltfläche **[Open]** und dann auf die Schaltfläche **[Import configuration file]**.
Abschnitt **Exportieren Konfiguration**	Um eine Konfiguration in eine XML-Datei zu exportieren, markieren Sie das oder die gewünschten Kästchen (Alle, Tresorkonfiguration, Einbruchskonfiguration, Übertragungskonfiguration) und klicken Sie dann auf die Schaltfläche **[Export configuration file]**.
Abschnitt **Download exportierte Konfiguration**	Am Ende des Exportierens einer Konfiguration klicken Sie auf die Schaltfläche **[Download]**, um die Konfigurationsdatei im XML-Format abzurufen und diese Datei dann in einem Kundenordner zu speichern.

4. Deaktivieren Sie den Wartungsport (siehe *Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS"*), da es eine Sicherheitslücke darstellt, einen Wartungsport offen zu lassen.

3.2.4.3. Verlängerung der Gültigkeitsdauer eines Tokens

Vor dem Ablauf des Tokens, das die Sicherheit des IP-basierten Austauschs zwischen TILLYS innerhalb einer Multi-TILLYS-Gruppe verwaltet, wurde ein Besuch der technischen Wartung vorgesehen, um eine teilweise Unterbrechung des Dienstes zu vermeiden.

Um die Gültigkeitsdauer eines Tokens zu verlängern, erstellen Sie ein neues Token und weisen Sie es dem TILLYS Gerät zu, dessen Token abläuft (siehe *Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät"*).

Kapitel 4. Installation, Einstellung und Verwendung des Terminals TACTILLYS-IP CUBE

4.1. Installation, Konfiguration und Wartung eines TACTILLYS-IP CUBE-Terminals

Diese Operationen werden von dem **Partner** TIL TECHNOLOGIES durchgeführt.

4.1.1. Physische Installation und Verbindung eines TACTILLYS-IP CUBE-Terminals

Einige Details zur physischen Installation und die technischen Daten finden Sie im *Datenblatt des TACTILLYS-IP CUBE-Terminals*.

1. Befestigen Sie die Halterung des TACTILLYS-IP in horizontaler Position an der Wand.
2. Schließen Sie ein RJ45-Kabel an die Rückseite des TACTILLYS-IP an.
3. Stecken Sie ein Lesegerät für Ausweise LEC05XF0200-NB6 in einen der beiden Anschlüsse am TACTILLYS-IP.
4. Schließen Sie an der Rückseite des TACTILLYS-IP ein Stromkabel für Gleichstrom an.
5. Befestigen Sie den TACTILLYS-IP an seiner Wandhalterung.
6. Verbinden Sie das RJ45-Kabel des TACTILLYS-IP mit dem Ethernet-Netzwerk.
7. Verbinden Sie das Stromkabel des TACTILLYS-IP mit einer 12-28 V DC-Stromversorgungsklemme. Das Display des TACTILLYS-IP schaltet sich ein und das TACTILLYS-IP startet.

Wenn der Alarm für den Manipulationsschutz ausgelöst wird, während das TACTILLYS-IP noch nicht an der Wandhalterung befestigt ist, siehe *Abschnitt 4.2.5, „Abstellen des Alarms für den Manipulationsschutz in der Installationsphase des TACTILLYS-IP CUBE“*.

Es ist auch möglich, die Stromversorgung des TACTILLYS-IP aus- und wieder einzustecken. Dies führt jedoch zu einem Neustart des TACTILLYS-IP (und unterbricht einen eventuell laufenden Einrichtungsvorgang).

4.1.2. Zutritt zur Schnittstelle für den Administrator des TACTILLYS-IP CUBE-Terminals und Anzeige der Produktmerkmale

1. Besorgen Sie sich den Netzwerk-Adressierungsplan, um eine verfügbare IP-Adresse für den TACTILLYS-IP CUBE zu finden.
2. Öffnen Sie auf einem tragbaren PC, der mit dem Ethernet-Netzwerk verbunden ist, einen Browser und geben Sie die Standard-IP-Adresse des TACTILLYS-IP CUBE ein: 172.16.5.240.

3. Geben Sie den Standard-Login und das Passwort für den Zutritt ein (admin/admin). Der Startseite-Bildschirm (Overwiew) wird angezeigt. Er enthält Informationen zur Konfiguration des TACTILLYS-IP.

   Sie können diesen Bildschirm jederzeit aufrufen, indem Sie auf das TACTILLYS-IP-Logo oben auf dem Bildschirm klicken oder auf das Symbol burger klicken und dann **System information > Overview** folgen.

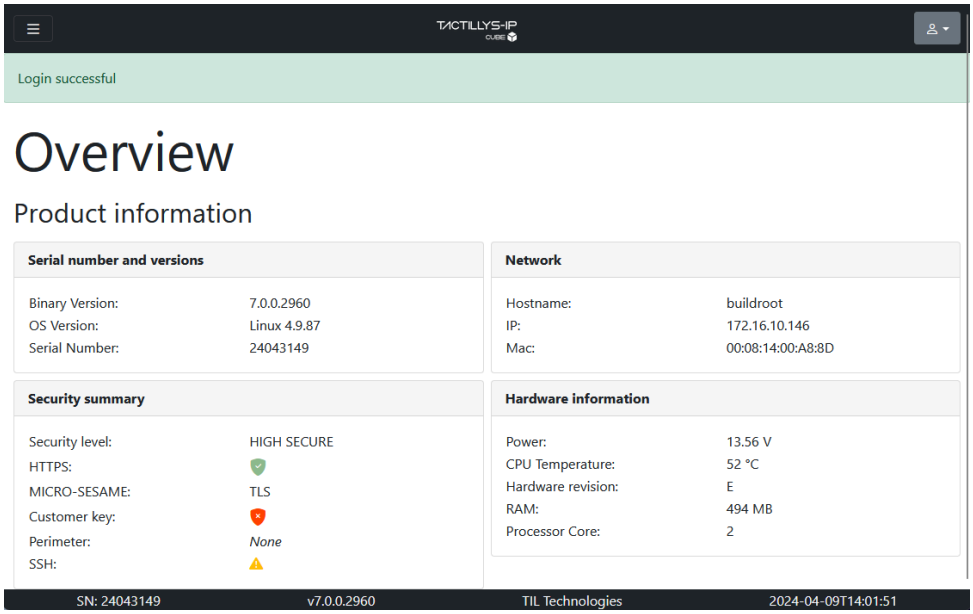

Abbildung 4.1. Startseite des TACTILLYS-IP (10010-028)

4.1.3. Änderung des Passworts für den Administrator des TACTILLYS-IP CUBE-Terminals

1. Von der Schnittstelle zum Administrator des TACTILLYS-IP CUBE aus, klicken Sie oben rechts auf dem Bildschirm auf das Symbol User und folgen **Sie** den **User settings**.

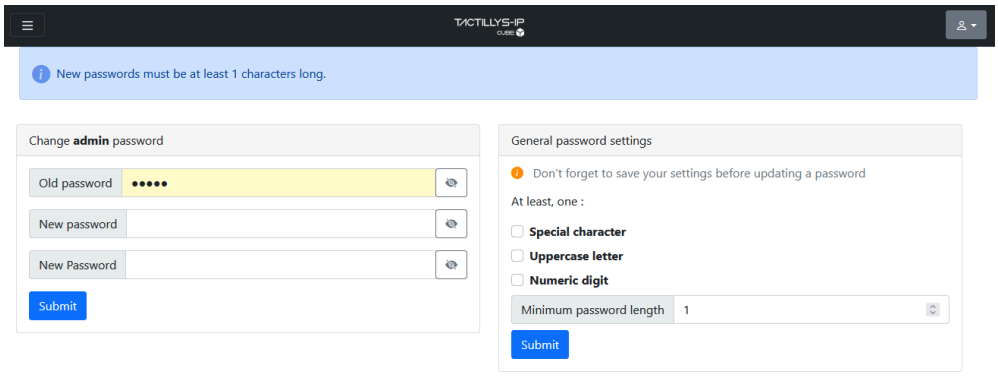

Abbildung 4.2. Startseite des TACTILLYS-IP CUBE (10010-029)

2. Geben Sie in die beiden Felder **New password** (siehe Abbildung unten) unbedingt ein neues Passwort ein, um das Standardpasswort zu ersetzen (und notieren Sie es an einem sicheren Ort, um seine Sicherheit zu gewährleisten).
3. Klicken Sie auf die Schaltfläche **[Submit]** im linken Bereich des Bildschirms.

Bevor Sie ein neues Passwort wählen, können Sie im Abschnitt rechts auf diesem Bildschirm die Sicherheitsstufe für das Passwort festlegen, die mit der Sicherheitsstufe des Standorts übereinstimmt (Sonderzeichen, Großbuchstaben, Zahlen und Länge des Passworts). Dieser Abschnitt hat eine eigene **[Submit]** - Schaltfläche.

4.1.4. Einstellen der Uhrzeit des Terminals TACTILLYS-IP CUBE

Die Uhrzeit wird nicht von einem externen NTP-Server verwaltet. Bei einem Neustart oder einer Neukonfiguration wird sie hingegen von der TILLYS in das zugehörige TACTILLYS-IP CUBE-Terminal heruntergeladen.

Sie muss bei der Inbetriebnahme des TACTILLYS IP eingestellt werden, um die Zertifikate zu installieren.

Wenn die Uhren von TACTILLYS-IP und *TILLYS* leicht voneinander abweichen, wird die Zeit berücksichtigt, zu der TILLYS die Nachrichten empfängt, oder die Zeit, zu der TILLYS den Standort scharf oder unscharf schaltet.

Bei der Umstellung auf Sommer- oder Winterzeit steuert der TACTILLYS-IP CUBE die Zeitumstellung.

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol burger in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Datum & Zeit.**
2. Geben Sie das Datum ein, geben Sie die Uhrzeit ein und klicken Sie dann auf die Schaltfläche **[Submit]**. Das eingegebene Datum und die Uhrzeit werden in der Statusleiste unten rechts auf dem Bildschirm angezeigt.

4.1.5. Netzwerk-Einstellungen des TACTILLYS-IP CUBE

Um Adressenkonflikte beim Hinzufügen mehrerer TACTILLYS-IP CUBEs zu vermeiden und aus Sicherheitsgründen sollte die Standardadresse des TACTILLYS IP nicht beibehalten werden.

Es ist auch möglich, die Netzwerkeinstellungen vom TACTILLYS-IP CUBE Einbruchsterminal aus zu ändern: siehe *Abschnitt 4.2.4, „Auswahl der Netzwerkeinstellungen des TACTILLYS-IP CUBE“*.

1. Von der Schnittstelle für den Administrator des TACTILLYS-IP CUBE aus klicken Sie auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Configuration > Network**.
2. Geben Sie mindestens denHostnamen (Hostname), die IP-Adresse (IP address), die Subnetzmaske (Subnet mask) und das Gateway (Gateway) ein und klicken Sie dann auf die Schaltfläche **[Submit]**.
3. Auf diesem Bildschirm können Sie im unteren Teil den TCP-Port für den Download (standardmäßig 20300) ändern, falls dieser *Port* für andere Anwendungen in Ihrem Netzwerk verwendet wird (im Zweifelsfall wenden Sie sich an den ISSD des Standorts).

4.1.6. Aktualisierung der Firmware des TACTILLYS-IP CUBE

Es ist immer eine gute Idee, die neueste Firmware in den TACTILLYS-IP CUBE zu laden.

1. Laden Sie *im Download-Bereich auf dem Standort des technischen Supports von TIL TECHNOLOGIES* die neueste Firmware für das Terminal TACTILLYS-IP CUBE herunter und legen Sie sie auf dem Desktop Ihres Computers ab.
2. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Firmware Upload**.
3. Klicken Sie auf die Schaltfläche **[Browse]** und wählen Sie auf dem Desktop die Firmwaredatei aus, die auf die TACTILLYS IP **geladen** werden soll, validieren Sie und klicken Sie dann auf die Schaltfläche **[↑ Upload and flash firmware]**. Dieser Vorgang dauert mehrere Minuten, dann wird TACTILLYS-IP neu gestartet.

4.1.7. Einrichten der Ereignisprotokollierung für den TACTILLYS-IP CUBE

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Log tracer.**
2. Um das Protokoll an eine bestimmte IP-Adresse zu senden, geben Sie diese IP-Adresse und den Zielport (standardmäßig 514) ein, klicken Sie auf den Syslog-Schalter (grau > blau) und klicken Sie dann auf die Schaltfläche **[Submit]**.

   Um das Protokoll in einer Datei zu speichern, klicken Sie auf den Syslog-Schalter (grau > blau) und dann auf die Schaltfläche **[Submit]**.

   Es ist möglich, beide Schalter zu aktivieren.

3. Wählen Sie die Detailstufe für die 7 Spurentypen aus und klicken Sie auf die Schaltfläche **[Submit]**.

4.1.8. Desetzen des TACTILLYS-IP CUBE

Bei dieser Wartung werden die standortspezifischen Schlüssel aus einem TACTILLYS-IP CUBE gelöscht. Sie sollte nur durchgeführt werden, wenn ein TACTILLYS-IP CUBE aus einer Installation entfernt wird, um ihn in einer anderen zu installieren, oder bevor er an die TIL TECHNOLOGIES SAV geschickt wird (auf Anfrage der Abteilung Kundenservice).

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Erase keys**.
2. Klicken Sie auf die Schaltfläche **[Erase keys]**.

4.2. Parametrierung des Terminals TACTILLYS-IP CUBE

Diese Operationen werden auf dem Terminal TACTILLYS-IP CUBE von **Benutzern mit Einbruch-Rechten** durchgeführt.

Der Benutzer mit Einbruch-Rechten hält einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE Einbruch-Terminals.

Je nach Konfiguration muss er vielleicht zusätzlich einen Code eingeben (siehe *Abschnitt 3.2.2.3, „Auswahl des Modus für die Authentifizierung (Ausweis oder Ausweis + Code) an einem TACTILLYS-IP CUBE“*).

4.2.1. Authentifizierung und Navigation auf einem TACTILLYS-IP CUBE-Terminal

Um auf die Startseite des TACTILLYS-IP CUBE zugreifen zu können, muss ein Ausweis verwendet werden, der vom System zur Erkennung von Einbrüchen erkannt wird: siehe *Abschnitt 5.2, „Verfahren zur Vorbereitung eines CUBE Ausweises zur Verwaltung von Einbrüchen auf einem TACTILLYS-IP CUBE Terminal“*.

1. Im Standby-Modus wird auf dem TACTILLYS-IP CUBE-Terminal die Nachricht "Halten Sie Ihren Ausweis an das Lesegerät" angezeigt.
2. Halten Sie einen Ausweis vor das Lesegerät (und geben Sie ggf. den Zugangscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.

   Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf diesem Bildschirm.

Piktogramm	Bedeutung
	Uhrzeit der nächsten Scharfschaltung
	Zutrittsverzug oder Austrittsverzug

Piktogramm	Bedeutung
	1 = Ausnahmegenehmigung läuft
	1 = Voralarm läuft
	Bewaffnete Gruppe
	Unbewaffnete Gruppe
	Anzeige der Gruppendetails (grünes Piktogramm)
	Scharfschaltung bereit
	Bewaffnung nicht bereit
	Anzeige der Übersicht über die Alarme

Tabelle 4.1. Bedeutung der Piktogramme auf dem Bildschirm der Gruppenliste auf dem Terminal TACTILLYS-IP CUBE

3. Berühren Sie das grüne Piktogramm  Lupe.

   Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Bildschirm mit den Details einer Gruppe.

Piktogramme an den Meldern	Bedeutung
	Auswurfstatus (orange = ausgeworfen)
	Sperrung (orange = gehemmt)
	Zutrittsverzug oder Austrittsverzug (orange = Verzögerungszeit läuft)
	1 = Ausnahmegenehmigung läuft
	Alarmzustand (orange = Alarm, rot = Selbstschutz)

Tabelle 4.2. Bedeutung der Piktogramme der Melder auf dem Terminal TACTILLYS-IP CUBE

4. Berühren Sie die Schaltfläche **[Sirenen]**.

   Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Display der Sirenen.

Piktogramme auf dem Sirenenbildschirm	Bedeutung
	Alarm-Status (orange = Alarm aktiv)

Piktogramme auf dem Sirenenbildschirm	Bedeutung
	Sperrung (orange = gehemmt)

Tabelle 4.3. Bedeutung der Sirenenpiktogramme auf dem Terminal TACTILLYS-IP CUBE

5. Um den Bildschirm mit den Meldern wieder anzuzeigen, berühren Sie die Schaltfläche **[Melder]**.

   Um den Startseite-Bildschirm wieder anzuzeigen, berühren Sie die Schaltfläche **[#]**, unten links auf dem Bildschirm.

   Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Bildschirm "Auswurf", der angezeigt wird, wenn ein Melder einen Fehler aufweist.

Piktogramme auf dem Auswurf-Bildschirm	Bedeutung
	Auswurfstatus (orange = ausgeworfen)
	Anzeige des aktuellen Fehlerstatus (orange = Alarm, rot = Selbstschutz)

Tabelle 4.4. Bedeutung der Piktogramme für den Auswurf eines Melders auf dem Terminal TACTILLYS-IP CUBE

4.2.2. Abfrage der Betriebsmerkmale von TACTILLYS-IP CUBE

Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Über**.

Die Betriebsmerkmale des TACTILLYS-IP CUBE werden angezeigt.

4.2.3. Parametrierung des TACTILLYS-IP CUBE

Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.

Die Helligkeit des Bildschirms ist einstellbar, ebenso wie die Lautstärke.

Es gibt 4 Themen und die Schnittstelle ist auf Deutsch, Englisch und Französisch verfügbar.
Die neuen Einstellungen werden übernommen, ohne dass eine Validierung oder ein Neustart erforderlich ist.

4.2.4. Auswahl der Netzwerkeinstellungen des TACTILLYS-IP CUBE

1. Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Netzwerk**.
2. Ändern Sie die Informationen und berühren Sie dann die Schaltfläche **[Speichern]**.

4.2.5. Abstellen des Alarms für den Manipulationsschutz in der Installationsphase des TACTILLYS-IP CUBE

Während der Einrichtungsphase, in der das Einbruchsterminal noch nicht in seiner Halterung befestigt ist und einen Alarm zum Manipulationsschutz auslösen kann, ist es möglich, den Positionssensor zurückzusetzen (wodurch auch der Alarm gestoppt wird).

1. Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.
2. Zeigen Sie den unteren Teil dieses Bildschirms an, indem Sie mit dem Finger nach unten scrollen, und berühren Sie dann rechts neben der Option **Position** die Schaltfläche **[Neu kalibrieren].**

4.2.6. Automatisches Abmelden des TACTILLYS-IP CUBE

Die Zeitverzögerung für den Übergang in den Standby-Modus kann auf dem Bildschirm **Einstellungen** des TACTILLYS-IP CUBE eingestellt werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittcode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt.
2. Tippe auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.
3. Wählen Sie den gewünschten Wert in der Drop-Down-Menüleiste **Standby** aus.

4.3. Verwendung des TACTILLYS-IP CUBE

Je nach Konfiguration und Komplexität der Standorte werden ein oder mehrere TACTILLYS-IP CUBE-Terminals installiert (siehe *Abschnitt 1.2, „Überblick über die Multi-TILLYS-Version des CUBE Einbruchs“*).

4.3.1. Manuelles Scharf- oder Unscharfschalten einer Gruppe

Die Scharfschaltung einer Gruppe erfolgt normalerweise zu der eingestellten Zeit. Bei einem Fehler an einem Melder, dessen automatischer Auswurf nicht vorgesehen ist, kann die Gruppe nicht scharf geschaltet werden.

Wenn ein Mitarbeiter am Wochenende kurz auf das Firmengelände zurückkehren muss, kann er den Alarm vorübergehend unscharf schalten. Es ist möglich, dass diese sich automatisch wieder scharf stellt, damit sie nicht vergessen wird und das Gebäude für den Rest des Wochenendes unbewacht bleibt.

Wenn ein Alarm ausgelöst wird, wird ein Sicherheitsbeamter den Melder überprüfen. Wenn es sich um eine technische Fehlfunktion handelt, kann er anschließend den manuellen Auswurf des

fehlerhaften Melders vornehmen, bevor er die Scharfschaltung der Gruppe erneut startet (siehe *Abschnitt 4.3.2, „Manueller Auswurf von fehlerhaften Meldern“*).

Das Scharf- und Unscharfschalten ist über MICROSESAME in der Übersicht (siehe *Abschnitt 5.5, „Übersicht auf MICROSESAME ansehen“*) oder über das Terminal TACTILLYS-IP CUBE möglich.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittcode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Berühren Sie die Gruppe, die Sie scharf/unscharf schalten möchten, und dann die Schaltfläche **[Scharf]** oder **[** Unscharf **]**.

4.3.2. Manueller Auswurf von fehlerhaften Meldern

Ein fehlerhafter Melder, dessen automatischer Auswurf nicht vorgesehen ist, kann in der Übersicht (siehe *Abschnitt 5.5, „Übersicht auf MICROSESAME ansehen“*) oder am TACTILLYS-IP CUBE Terminal ausgeworfen werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittcode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Tippe auf das Symbol burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Auswerfen**.
3. Berühren Sie den fehlerhaften Melder (Piktogramm ⚠ orange oder rot) und dann die Taste **[Auswerfen]**.

4.3.3. Sirenen ausschalten

Eine Sirene kann in der Übersicht (siehe *Abschnitt 5.5, „Übersicht auf MICROSESAME ansehen“*) oder am TACTILLYS-IP CUBE Terminal gestoppt werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittcode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Berühren Sie das grüne Piktogramm 🔍 Lupe der Gruppe mit der Sirene, die Sie abschalten möchten.
3. Berühren Sie die klingelnde Sirene (Piktogramm ⚠ orange oder rot) und dann die Taste **[Sirenenstopp]**.

4.3.4. Überschreiben der Scharfschaltung auf Meldergruppe(n)

Die Scharfschaltung einer Gruppe kann so programmiert werden, dass sie automatisch zu einer bestimmten Uhrzeit erfolgt. Allerdings kann es vorkommen, dass die Nutzer nach der

Überwachungszeit noch vor Ort bleiben müssen, sodass sie die Überwachungszeit um die Zeit verschieben müssen, die sie benötigen.

Aus Sicherheitsgründen kann diese Zeit jedoch begrenzt werden, z. B. durch den Sicherheitsbeauftragten.

Wenn der *Voralarm* ertönt, müssen die Personen, die sich noch in den Räumlichkeiten befinden, diese vor Ablauf der Ausgehzeit verlassen oder sich, falls sie dazu berechtigt sind, am Terminal TACTILLYS-IP CUBE identifizieren und eine Ausnahmegenehmigung beantragen.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittcode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Berühren Sie die Gruppe, für die Sie eine Ausnahme beantragen möchten, und dann die Schaltfläche **[Überschreiben]**.
3. Wählen Sie die Dauer der Überschreibung und validieren Sie.

Kapitel 5. Konfiguration und Nutzung des CUBE-Einbruchs

Diese werden vom **Sicherheitsbeauftragten** durchgeführt.

5.1. Importieren der CUBE Einbruch-Konfiguration in MICROSESAME

Im Falle einer Multi-TILLYS-Konfiguration müssen alle *TILLYS*(LVE) in *MICROSESAME* bekannt sein. Daher ist ein vollständiger Download erforderlich.

1. In der Startseite von MICROSESAME folgen Sie **Einstellungen > Hardware > Lokale Verarbeitungseinheit [LVE]**.
2. Doppelklicken Sie auf den Namen des TILLYS, dessen Einstellungen importiert werden sollen.

Abbildung 5.1. Vorbereiten des Imports der Einbruch-Konfiguration eines TILLYS in MICROSESAME (10010-038)

3. Geben Sie den Namen und das Passwort ein (1), überprüfen Sie die Sicherheitsstufe (2) und klicken Sie auf die Schaltfläche **[+ Fügen Sie eine Funktion hinzu]** (3).
4. Klicken Sie in der Drop-Down-Menüleiste auf **Einbruch CUBE**.
5. Klicken Sie auf der rechten Seite des Bildschirms auf die Schaltfläche **[CUBE Einbruch-Konfiguration importieren]**.

5.2. Verfahren zur Vorbereitung eines CUBE Ausweises zur Verwaltung von Einbrüchen auf einem TACTILLYS-IP CUBE Terminal

Ein Partner von TIL Technologies, ein Empfangsmitarbeiter oder ein Sicherheitsbeauftragter bereitet einen Ausweis für den Zutritt zum TACTILLYS-IP CUBE Anti-Einbruchsterminal in MICROSESAME vor, indem er die in den folgenden Abschnitten beschriebenen Schritte ausführt.

5.2.1. Vorbereitung eines Ausweises zur Kontrolle gegen Einbrüche

Die Erfassung eines ID-Mittels in MICROSESAME im Schritt *Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »* erfolgt, indem ein Ausweis an einem Lesegerät zur Zutrittskontrolle vorbeigeführt wird.

Das im Terminal TACTILLYS-IP CUBE integrierte Lesegerät ist kein Lesegerät für die Zutrittskontrolle, sondern ein Lesegerät für den Einbruchschutz.

5.2.2. Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Überwachung > Ereignismonitor [MON]**.
2. Einen nicht zugewiesenen Ausweis vor das Lesegerät für die Zutrittskontrolle halten. Ein akustisches Signal zeigt an, dass das Lesegerät funktioniert, aber der Zutritt ist abgelehnter Zutritt, da der Ausweis unbekannt ist (er wurde noch nicht zugewiesen).
   Sein ID-Mittel wurde von MICROSESAME erworben (es ist im Ereignismonitor sichtbar) und steht für einen neuen Benutzer zur Verfügung.
   Wenn das Lesegerät kein akustisches/visuelles Signal ausgibt, wenden Sie sich unter Fehlerbehebung zu den Fehler 00003.
3. Klicken Sie auf das Symbol **[Details]** in der linken oberen Ecke des Bildschirms. Die Details des Ausweises werden im rechten Fenster angezeigt.
4. Rechts neben dem Ort des Fotos markieren Sie die ID-Mittel mit der Maus und geben Sie **STRG + C** ein. Die ID-Mittel wird in den Speicher kopiert: weiter *Section 5.2.3, « Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer »*.

5.2.3. Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Klicken Sie oben links auf **Hinzufügen**, geben Sie den Vor- und Nachnamen des neuen Users ein und klicken Sie dann auf **Erstellen**.
3. Klicken Sie auf **ID-Mittel**, machen Sie **einen** Rechtsklick im unteren Bildschirmbereich und klicken Sie auf **ID-Mittel erstellen**.

4. Tippen Sie **CRTL + V** ein. Die kopierteID-Mittel (siehe *Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »*) wird in die Spalte Code eingefügt.
5. Geben Sie ein Start- und Enddatum für die Gültigkeit ein und klicken Sie auf Enter.
6. Klicken Sie auf **Speichern** : Das Hochladen dieser Informationen in den TILLYS wird durchgeführt.
7. Gehen Sie im Hauptmenü auf **Nutzung > Überwachung > Ereignismonitor [ERE]** (Anzeige des **Ereignismonitors**) und halten Sie den Ausweis vor das Lesegerät.
   Der Ausweis ist nun mit dem Namen der Person verknüpft, die Sie eingegeben haben, aber sein Zustand ist immer noch abgelehnter Zutritt (kein Zugriff auf das Lesegerät), und das ist völlig normal, da er noch nicht mit Zugriffsrechten verknüpft ist.
   Er besitzt auch kein CUBE Einbruchsprofil, das ihm den Zugriff auf ein TACTILLYS-IP CUBE Terminal ermöglicht.

5.2.4. Zuweisung von Zutritten an einen neuen Benutzer

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Suchen Sie nach dem zuvor erstelltenUser.
3. Klicken Sie in seiner Datei auf **Zutritt**.
4. Im unteren rechten Bereich klicken Sie auf
5. Klicken Sie in der sich öffnenden Liste auf **Alle aktuellen und zukünftigen Standorte**.
6. Klicken Sie im daraufhin angezeigten Fenster für die Zugriffseinstellungen auf **OK** (Validierung des 24-Stunden-Zugriffs).
7. Klicken Sie auf **Speichern** .
8. Rufen Sie den **Ereignismonitor** auf (im Hauptmenü unter **Betrieb > Überwachung > Ereignismonitor [ERE]**), halten Sie den Ausweis vor jedes zuvor zugewiesene Lesegerät und überprüfen Sie, dass der Benutzer nicht nur erkannt wird, sondern dass ihm nun auch der Zugang gewährt wird.

5.2.5. Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen

Die Benutzer, die mit der Verwaltung eines TACTILLYS-IP CUBE-Terminals beauftragt sind, müssen mindestens über das Einbruchsprofil verfügen, das diesem Terminal entspricht.

Sie müssen auch über Zutrittsrechte zum Gebäude an den Lesegeräten für die Zutrittskontrolle verfügen.

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Suchen Sie nach dem zuvor erstelltenUser.
3. Klicken Sie in seiner Datei auf **Zutritt**.
4. Im unteren rechten Bereich klicken Sie auf

5. Klicken Sie auf das Burger-Menü in der Mitte der rechten Bildschirmhälfte und markieren Sie dann das Kontrollkästchen CUBE Einbruchsprofile anzeigen.
6. Klicken Sie im rechten Abschnitt auf das Einbruchsprofil. Klicken Sie auf den Pfeil <, um dieses Profil in den linken Abschnitt des Bildschirms zu verschieben.
7. Weisen Sie auf die gleiche Weise die Zutrittsrechte zum Gebäude zu, die dieser ID-Mittel benötigt.
8. Klicken Sie auf **Speichern** .
9. Im Hauptmenü folgen Sie **Einstellungen > Hardware > Lokale Verarbeitungseinheiten [LVE]**.
10. Doppelklicken Sie auf die Linie der TILLYS(LVE), die mit der TACTILLYS verbunden ist.
11. Klicken Sie auf die Schaltfläche , dann auf die Schaltfläche .
12. Markieren Sie das Feld Zutritt und klicken Sie auf die Schaltfläche **[Ausführen]**.

5.3. Verwaltung der Einbruchsprofile der Benutzer auf MICROSESAME oder WEBSESAME

Einbruchsprofile können zu den Zutrittsprofilen der Benutzer hinzugefügt werden.

Sie können auch durch das Importieren von CSV-Dateien im richtigen Format verwaltet werden, die von den Personalabteilungen gemäß den von der Organisation, die das Anti-Einbruch-System verwendet, eingerichteten Prozessen vorbereitet wurden.

Siehe *Abschnitt 3.2.2.1, „Erstellen von Einbruchsprofilen auf der Host-TILLYS“*.

5.4. Einrichten der Übersicht auf MICROSESAME

Ähnlich wie Tür-Objekte die Zutrittskontrolle durch ihre grafische Darstellung vereinfachen, vereinfachen Überwachungsobjekte das Management von Einbrüchen.

1. In der Startseite von MICROSESAME folgen Sie **Einstellungen > Überwachung > Übersichtseditor [EDI].**
2. Ziehen Sie die Einbruch-Objekte (Melder, Sirenen, TILLYS) aus dem rechten Fenster in den mittleren Bereich an die gewünschte Stelle auf der Grafik oder fotografischen Darstellung des Standorts.
3. Für jedes dieser Objekte kann man auf die drei übereinander liegenden Punkte (rechts oben in jedem Objekt) klicken, um Optionen anzuzeigen. Um die Ereignisse eines Einbruch-Objekts zu erhalten, markiere dessen **Verlaufsfeld**.

   Weitere Informationen finden Sie im Abschnitt über den Übersichtseditor im *MICROSESAME-Referenzhandbuch*.
4. Speichern Sie die Konfiguration.

5.5. Übersicht auf MICROSESAME ansehen

Siehe den Abschnitt über die Anzeige von Übersichten im *MICROSESAME-Referenzhandbuch*.

5.6. Erklärung der Operatoren für die Erkennung von Einbrüchen auf der TILLYS

Sobald die Einbruchsprofile definiert und diese Konfiguration auf MICROSESAME geladen wurde, können Sie den Personen, die die Scharf- und Unscharfschaltung des Alarms auf dem TACTILLYS-IP CUBE-Terminal verwalten sollen, ein Einbruchsprofil zuweisen.

Siehe *Abschnitt 5.3, „Verwaltung der Einbruchsprofile der Benutzer auf MICROSESAME oder WEBSESAME“*.

5.7. Test der Anlage zur Erkennung von Einbrüchen

5.7.1. Testen von Meldern

1. Klicken Sie auf das Symbol  burger in der oberen linken Ecke des TILLYS-Host-Bildschirms und folgen Sie **Einbruch CUBE > Detector diagnostic**.
2. Bewegen Sie sich in allen Räumen des Gebäudes, in denen ein Melder installiert ist (der Alarm wird nicht ausgelöst).
3. Überprüfen Sie im Ereignisticker, ob alle Melder reagiert haben.
4. Den Modus Detector diagnostic deaktivieren.

5.7.2. Test der Kommunikation zwischen TILLYS und dem TACTILLYS-IP CUBE

Wenn die Verbindung zwischen dem TILLYS und dem Terminal TACTILLYS-IP CUBE funktioniert, aktiviert das Auflegen eines Ausweises mit Einbruchfunktion auf das Lesegerät des Terminals TACTILLYS-IP CUBE dessen Startseite (oder dessen Codeeingabebildschirm).

Kapitel 6. Sicherheitsmanagement durch den Sicherheitsbeauftragten

6.1. Zuweisung von Zutritten an die Benutzer des TACTILLYS-IP CUBE

Dieser Abschnitt schlägt lediglich eine alternative Formulierung vor: siehe *Section 5.2.5, « Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen »* oben.

6.2. Änderung des ID-Mittels Einbruch, das bei der Ausweis- und Code-Identifikation auf TACTILLYS-IP CUBE verwendet wird.

Die Änderung des ID-Mittels wird in MICROSESAME vorgenommen. Darauf folgt ein manueller Download in die TILLYS.

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Klicken Sie auf den Reiter Zugang, wählen Sie das Zutrittsprofil aus und klicken Sie auf die Schaltfläche **[ID-Mittel]**.
3. Scrollen Sie nach unten und sehen Sie sich den vorhandenen Code an oder geben Sie einen neuen Code ein und klicken Sie dann auf Speichern.
4. Zur Auswahl des Modus für die Authentifizierung siehe *Abschnitt 3.2.2.3, „Auswahl des Modus für die Authentifizierung (Ausweis oder Ausweis + Code) an einem TACTILLYS-IP CUBE“*.

6.3. Abfrage des Verlaufs von Einbrüchen

MICROSESAME- oder WEBSESAME-Operatoren loggen sich in die webbasierte Schnittstelle des Host-TILLYS ein.

Kapitel 7. Operationen im Zusammenhang mit dem Einbruch, die vom Fernüberwachungsmonitor durchgeführt werden

7.1. Abfrage der aktuellen Alarme

Der Fernüberwachungsmonitor kann die Details der aktuellen Alarme auf seinem Terminal einsehen.

Die Informationen, die er erhält, ermöglichen es ihm auch, das reibungslose Funktionieren der Verbindung zu überwachen (siehe *Abschnitt 7.1.1, „Syntax von Polling-Nachrichten“* und *Abschnitt 7.1.2, „Syntax der Nachrichten zum zyklischen Test“*).

7.1.1. Syntax von Polling-Nachrichten

Polling ist eine Testnachricht, die von TILLYS alle paar Sekunden gesendet wird, um zu überprüfen, ob die IP-Übertragungsfunktion zwischen TILLYS und dem Fernüberwachungs-Frontend ordnungsgemäß funktioniert. Er wird dann an den Fernüberwachungsmonitor weitergeleitet.

Beispiel für eine Polling-Nachricht

```
E99B0013"NULL"0004L0#7005[]
```

Diese Testnachricht enthält eine Nachricht vom Typ "NULL", die keine Daten enthält.

Informationen zum Aktivieren und Konfigurieren von Polling finden Sie unter *Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“*.

7.1.2. Syntax der Nachrichten zum zyklischen Test

Der zyklische Test ist eine Testnachricht, die von der TILLYS gesendet wird, um zu überprüfen, ob die IP-basierte Übertragungsfunktion zwischen der TILLYS und jedem Fernüberwachungsmonitor ordnungsgemäß funktioniert. Er wird z. B. alle 3 Stunden (180 Minuten) aktiviert.

Beispiel für eine Nachricht über einen zyklischen Test

```
4558001F"SIA-DCS"0001L0#7005[#7005|NRP]
```

In dieser Nachricht steht N für neu und RP für den Ereigniscode, der den zyklischen Test bezeichnet.

Informationen zum Aktivieren und Konfigurieren des zyklischen Tests finden Sie unter *Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“*.

7.2. Fernbefehl Einbruch CUBE

Zusätzlich zum Telefonanruf des Standorts, der Polizei oder der Feuerwehr kann der Fernüberwachungsmonitor die unten aufgeführten Aktionen durchführen.

7.2.1. Scharfstellung

Dies ist zwar möglich, kommt aber praktisch nie vor, da es schwierig ist, aus der Ferne zu überprüfen, ob die Räume leer sind.

7.2.2. Sirenenstopp

Der Fernüberwachungsmonitor kann die Sirenen ausschalten, nachdem er die Alarme quittiert hat.

7.2.3. Abrüstung

Der Fernüberwachungsmonitor kann eine Gruppe bei Bedarf aus der Ferne entschärfen.

7.2.4. Änderung des Wertes eines Registers der TILLYS

Diese Funktion ist nur verfügbar, wenn das Frontend des Fernüberwachungsmonitors und die Überwachungssoftware des Fernüberwachungsmonitors mit dieser Änderung des Registers kompatibel sind.